Kúpna zmluva č. 27/2024

uzatvorená podľa § 409 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ďalej len „Obchodný zákonník") a zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO")

ČI. 1
Zmluvné strany

Kupujúci:

Názov:	mestská časť Bratislava-Staré Mesto
Sídlo:	Vajanského nábrežie 3, 814 21 Bratislava
IČO:	00 603 147
Bankové spojenie:	VÚB, a. s.
IBAN:	SK02 0200 0000 0000 0152 6012
V zastúpení:	Ing. Matej Vagač, starosta

ďalej len „objednávateľ"

a

predávajúci:

Obchodné meno:	CSFIT s.r.o.
Sídlo:	Galvaniho 7/D, 821 04 Bratislava
IČO:	50 700 308
IČ DPH:	SK2120439794
Obchodný register:	Obchodný register Mestského súdu Bratislava III, Sro, vložka č. 117399/B
Bankové spojenie:	Fio banka, a. s., pobočka zahraničnej banky Dunajská 1, 811 08 Bratislava
IBAN:	SK5383300000002701168809
Kontaktný e-mail:	obchod@csfit.sk
V zastúpení:	Ing. Pavol Jurčo, konateľ

ďalej len „dodávateľ"

ČI. 2
Úvodné ustanovenia

1. Táto kúpna zmluva sa uzatvára ako výsledok verejného obstarávania zákazky s nízkou hodnotou v zmysle § 117 ZVO vyhlásenej objednávateľom ako verejným obstarávateľom na predmet zákazky s názvom „Aktívne sieťové zariadenia na zvýšenie zabezpečenia siete v rámci procesov zavádzania súladu so Zákonom o kybernetickej bezpečnosti a poskytovanie profesionálnych služieb súvisiacich s dodávkou komponentov".
2. Dodávateľ je úspešným uchádzačom v procese verejného obstarávania na dodanie predmetu zákazky uvedeného v ods. 1 tohto článku zmluvy. Zmluvné strany týmto vyhlasujú, že sú spôsobilé túto zmluvu uzatvoriť a plniť záväzky z nej vyplývajúce.

Čl. 3
Predmet zmluvy

1. Predmetom tejto kúpnej zmluvy je záväzok dodávateľa v dohodnutom termíne a na dohodnutom mieste dodať a nainštalovať objednávateľovi predmet obstarávania v zložení:
   - 2 ks firewall značky Fortinet, typ FG-101F;
   - 2 ks core 24-portový switch značky Fortinet, typu FS-1024E;
   - 9 ks 48-portový switch značky Fortinet, typu FS-148F;
   - 4 ks 24-portový switch značky Fortinet, typu FS-124F;
   - 7 ks 8-portový switch značky Fortinet, typu FS-108F;
   - 1 ks SW monitorovanie a zhromažďovanie záznamov (VM) Fortinet FortiAnalyzer Virtual Appliances;
   - 2 ks balík SW klient pre vzdialené pripojenie značky FortiClient VPN/ZTNA Agent Subscription for 25 endpoints
   - Príslušenstvo (káble, optické moduly - podľa prílohy č. 1)

   (ďalej „predmet zmluvy") podľa technickej špecifikácie uvedenej v prílohe č. 1 tejto zmluvy. Príloha č. 1 je neoddeliteľnou súčasťou tejto zmluvy.
2. Predmetom tejto kúpnej zmluvy je aj poskytovanie profesionálnych služieb súvisiacich s dodávkou komponentov na zvýšenie zabezpečenia siete a pre segmentáciu siete v oblasti riadenia bezpečnosti sietí a informačných systémov pri zavádzaní súladu so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB") (inštalácia, konfigurácia, nastavenia, migrácia), podľa technickej špecifikácie uvedenej v prílohe č. 1 tejto zmluvy.
3. Predmetom kúpnej zmluvy je nový nepoškodený a neopravovaný, doposiaľ nepoužívaný tovar.
4. Dodávateľ je povinný zabezpečiť rozšírený 3 ročný záručný servis typu FortiCare Premium and FortiGuard Enterprise Protection 3Y v prípade firewalow a FortiCare Premium Support 3Y v prípade switchov a dodávaného sofvéru.
5. Objednávateľ sa zaväzuje od dodávateľa prevziať riadne a včas dodaný predmet zmluvy a zaplatiť kúpnu cenu.
6. Vlastnícke právo k predmetu zmluvy prechádza na objednávateľa jeho prevzatím.

Čl. 4
Kúpna cena

1. Kúpna cena za predmet zmluvy podľa tejto zmluvy je stanovená v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov dohodou, a predstavuje sumu 89.574,60 EUR bez DPH, t. j. sumu **107.489,52 EUR s DPH, slovom stosedemtisíc štyristoosemdesiatdeväť' euro päť'desiatdva centov s DPH.**
2. V kúpnej cene uvedenej v predchádzajúcom odseku je zahrnutá cena transportu predmetu zmluvy do miesta sídla objednávateľa ako aj všetky ostatné náklady súvisiace s riadnym plnením tejto zmluvy.

Čl. 5
Platobné podmienky

1. Kúpnu cenu podľa tejto zmluvy uhradí objednávateľ na základe faktúry dodávateľa. Faktúra musí obsahovať náležitosti podľa § 3a ods. 1 zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov a podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. Súčasťou faktúry bude dodací list podpísaný oprávneným zástupcom dodávateľa a oprávneným zástupcom objednávateľa, ktorí svojím podpisom potvrdia odovzdanie a prevzatie predmetu zmluvy v súlade so zmluvou. V prípade, že faktúra nebude obsahovať predpísané náležitosti, objednávateľ má právo vrátiť ju dodávateľovi v lehote splatnosti na doplnenie a prepracovanie. V takomto prípade sa preruší lehota splatnosti a nová

lehota splatnosti začne plynúť doručením opravenej resp. novej faktúry objednávateľovi.

2. Faktúra je splatná do 30 dní odo dňa jej doručenia objednávateľovi v zmysle Čl. 6 ods. 3.

Čl. 6
Lehota a miesto dodania, odovzdanie a prevzatie predmetu zmluvy

1. Dodávateľ sa zaväzuje dodať Objednávateľovi predmet zmluvy podľa Čl. 3 tejto Zmluvy v nasledovných termínoch:
   - Etapa 1 (dodávka komponentov, vrátane softvéru a príslušenstva): maximálne do 42 kalendárnych dní od účinnosti zmluvy;
   - Etapa 2 (poskytovanie profesionálnych služieb súvisiacich s dodávkou komponentov): maximálne do 30 kalendárnych dní od ukončenia Etapy 1.
2. Dodávateľ zabezpečí dodanie predmetu zmluvy do miesta sídla objednávateľa Vajanského nábrežie 3, 814 21 Bratislava.
3. Pri odovzdaní predmetu zmluvy je dodávateľ povinný odovzdať objednávateľovi akceptačný a preberací protokol, na ktorom oprávnení zástupcovia zmluvných strán potvrdia odovzdanie a prevzatie predmetu zmluvy.
4. Predmet Zmluvy sa považuje za dodaný podpísaním akceptačného a preberacieho protokolu, ktorým bude potvrdené odovzdanie a prevzatie predmetu zmluvy (Etapa 1 + Etapa 2).
5. Dodávateľ po ukončení inštalačných a konfiguračných prác odovzdá odberateľovi aj faktúru s náležitosťami podľa čl. 5 tejto zmluvy.
6. Dodávateľ je povinný zabaliť predmet zmluvy na prepravu tak, aby neprišlo k jeho poškodeniu.
7. V prípade, ak by mal predmet zmluvy pri odovzdaní viditeľné vady, ktoré by bránili v jeho riadnom užívaní, objednávateľ nie je povinný predmet zmluvy prevziať.
8. Nebezpečenstvo škody na predmete zmluvy prechádza na objednávateľa okamihom jeho prevzatia na základe podpísaného dodacieho listu oprávnenými zástupcami objednávateľa a dodávateľa podľa ods. 1 tohto článku.

Čl. 7
Záručná doba

1. Dodávateľ zodpovedá za to, že predmet zmluvy bude mať počas záručnej doby vlastnosti dohodnuté v zmluve.
2. Záručná doba na predmet zmluvy je 3 roky a začína plynúť odo dňa riadneho odovzdania a prevzatia predmetu zmluvy.
3. Dodávateľ zodpovedá za vady, ktoré má predmet zmluvy v čase jeho odovzdania objednávateľovi. Za vady, ktoré sa prejavili po odovzdaní predmetu zmluvy zodpovedá dodávateľ vtedy, ak boli spôsobené porušením jeho povinností.
4. Pri zodpovednosti za vady sa zmluvné strany budú riadiť ustanoveniami § 436 a nasl. Obchodného zákonníka, ktoré upravujú nároky zo zodpovednosti za vady.
5. V prípade, že sa počas záručnej doby zistí vada na predmete zmluvy, objednávateľ písomne upozorní dodávateľa na túto skutočnosť. Počas záručnej doby má objednávateľ právo požadovať a dodávateľ povinnosť bezplatne odstrániť zistené a reklamované vady. V prípade výmeny vadného predmetu zmluvy za nový bez vady, prestáva plynúť pôvodná záručná doba a začína plynúť nová záručná doba podľa ods. 2 tohoto článku.
6. Dodávateľ sa zaväzuje poskytnúť na predmet zmluvy aj pozáručný servis v prípade záujmu objednávateľa.

Čl. 8
Zmluvné sankcie a odstúpenie od zmluvy

1. Dodávateľ je povinný dodať predmet zmluvy v množstve a kvalite predpokladanej v podrobnom opise predmetu zákazky / podrobnej technickej špecifikácii a osobitnými požiadavkami na plnenie. V prípade nesplnenia tejto povinnosti vzniká objednávateľovi právo požadovať zaplatenie zmluvnej pokuty vo výške 30,- € za každý deň omeškania a za každú vadu dodaného plnenia samostatne a v prípade nesplnenia povinnosti uvedenej v tomto odseku ani v dodatočnej lehote 5 pracovných dní odo dňa, kedy malo dôjsť k riadnemu plneniu, je objednávateľ oprávnený od zmluvy okamžite odstúpiť. Zmluvnú pokutu uhradí dodávateľ na základe faktúry vystavenej objednávateľom.
2. Uplatnením nároku na zaplatenie pokuty, ani jej zaplatením nie je dotknuté právo objednávateľa na náhradu škody, ktorá mu porušením povinností dodávateľa vznikla.
3. Okrem uplatnených sankcií z omeškania podľa tejto zmluvy, majú zmluvné strany právo žiadať náhradu škody, ktorá im vznikla a bola spôsobená porušením, resp. zanedbaním povinností druhou zmluvnou stranou podľa tejto zmluvy.
4. Objednávateľ má právo od tejto zmluvy odstúpiť v prípade podstatného porušenia tejto zmluvy zo strany dodávateľa. Za podstatné porušenie tejto zmluvy zo strany dodávateľa sa považuje:
   A) ak je dodávateľ v omeškaní s plnením podľa Čl. 6 tejto zmluvy dlhšie ako 5 dní,
   B) ak predmet zmluvy nebude dodaný v súlade s Čl. 3 tejto zmluvy a podľa podmienok uvedených v tejto zmluve.
5. V prípade nedodržania splatnosti faktúry má dodávateľ právo požadovať úrok z omeškania podľa § 369 ods. 2 Obchodného zákonníka.

Čl. 9
Záverečné ustanovenia

1. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ďalšími všeobecne záväznými právnymi predpismi.
2. Všetky ďalšie zmeny a doplnky musia byť vyjadrené formou písomného očíslovaného dodatku podpísaného oprávnenými zástupcami zmluvných strán.
3. Zmluvné strany nie sú oprávnené previesť práva a/alebo záväzky vyplývajúce z tejto zmluvy na tretie osoby bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.
4. Spory zmluvných strán sa budú riešiť podľa právneho poriadku Slovenskej republiky a prostredníctvom príslušného súdu v Slovenskej republike.
5. Táto zmluva nadobúda platnosť dňom jej podpisu oprávnenými zástupcami zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv.
6. Táto zmluva je vyhotovená v troch rovnopisoch, z ktorých každá má platnosť originálu, pričom objednávateľ dostane dva rovnopisy a dodávateľ dostane jeden rovnopis.
7. Zmluvné strany vyhlasujú, že si zmluvu pred jej podpisom prečítali, s jej obsahom súhlasia, čo potvrdzujú svojim podpisom

Bratislava dňa .....

Objednávateľ

.....

mestská časť Bratislava-Staré Mesto
Ing. Matej Vagač, starosta

Bratislava dňa

Dodávateľ

.....

CSFIT s. r .o.
Ing. Pavol Jurčo, konateľ

Príloha č. 1 ku Kúpnej zmluve - Technická špecifikácia

Predmetom zákazky je dodávka a inštalácia komponentov (aktívnych sieťových zariadení) na zvýšenie zabezpečenia siete a pre segmentáciu siete v rámci oblasti riadenia bezpečnosti sietí a informačných systémov pri zavádzaní súladu so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej ako ZoKB). Komponenty sieťovej infraštruktúry musia tvoriť ucelenú funkčnú a bezpečnostnú infraštruktúru pre segmentáciu siete so 100% kompatibilitou medzi jednotlivými položkami. Požadované je riešenie od jedného výrobcu, kvôli jednotnému manažmentu. Uvedené zariadenia musia medzi sebou vedieť komunikovať, odovzdávať si časti konfigurácie a zabezpečovať ochranu IT infraštruktúry ako jeden prvok. Obstarávaná sieťová infraštruktúra musí zabezpečiť segmentáciu IT prostredia do menších logických prvkov s kontrolovanými prestupmi. Prístup k sieťovej infraštruktúre musí podporovať zabezpečenie, overovanie a autorizáciu pripájaných zariadení. Súčasťou zákazky bude softvérové riešenie na monitorovanie a zhromažďovanie záznamov z dodaných sieťových zariadení, ktoré budú na základe týchto záznamov analyzovať a vyhodnocovať bezpečnostné riziká. A softvérové riešenie pre bezpečný prístup pre vzdialených používateľov, využitím princípu nulovej dôveryhodnosti, ktorý sa zameriava na riadenie prístupu k aplikáciám – spĺňajúcu koncepciu Zero Trust Network Access (ZTNA).

Etapa 1 (dodávka komponentov, vrátane softvéru a príslušenstva):

Popis	**Jednotka**	**Minimum**	**Maximum**	**Presná hodnota**
Technické vlastnosti	**Hodnota / charakteristika**			
01. Firewall	*ks*			*2*
Technická špecifikácia:	HW zariadenie NGFW/UTM firewall; Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií;			
Celkový počet portov GE RJ45:	min. 22x GE RJ45 portov			
Hardvérovo akcelerované GE RJ45 Porty:	min. 12x			
Hardvérovo akcelerované GE RJ45 Management / HA / DMZ Porty:	min. 1x / 2x / 1x			
Hardvérovo akcelerované GE SFP Sloty:	min. 4x			
Hardvérovo akcelerované 10 GE SFP+ Sloty:	min. 2x			
GE RJ45 WAN Porty:	min. 2x			
GE RJ45 alebo SFP zdieľané Porty:	min. 4x			
USB Port :	min. 1x			
Konzolový Port (GE RJ45):	min. 1x			
Úložisko:	min. 1x 480 GB SSD			
IPS / Priepustnosť IPS:	✓, min. 2,6 Gbps			
Podpora VLAN:	✓, min. 4000			
Podpora LACP:	✓			
Počet FW pravidiel:	✓, min. 10000			
Možnosť definície FW pravidel v tzv. NGFW režime / Priepustnosť NGFW:	✓, min. 1,6 Gbps			
Threat Ochrana / Priepustnosť Threat Ochrany:	✓, min. 1 Gbps			
Počet virtuálnych domén (predvolené / Maximum):	10 / 10			
Celková priepustnosť firewallu:	min. 20 / 18 / 10 Gbps (merané na UDP paketoch s veľkosťou: 1518 B / 512 B / 64 B)			
Latencia firewallu (merané na UDP paketoch 64 B):	nepresahuje 5 µs			
Počet nových spojení za sekundu (setup-rate):	min. 55000			
Celkový počet súčasných TCP spojení firewallu:	min. 1 500 000			
PPS (počet spracovaných paketov za 1 sekundu):	min. 15 000 000			

Funkcia detekcie aplikácií na L7 (Application Control):	✓
Detekcia známych aplikácií na základe signatúr:	Min. 3300 preddefinovaných aplikácií/signatúr
Pre populárne cloud aplikácie sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login:	✓, min. Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn
Aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu:	✓
Priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response):	min. 2 Gbps
Podpora použitia Application control aj formou profilov priradených k pravidlám:	✓
Funkcie detekcie a zamedzenia narušení (IPS/IDS):	✓
Možnosť detekcie a zamedzenie narušení (IPS/IDS) pre IoT zariadenia:	✓
Funkcia ohodnodnotenia celkovej úrovne bezpečnosti tzv. Security Rating:	✓
Funkcia umožňujúca zabránenie úniku dát tzv. DLP:	✓
Funkcia detekcie neznámych škodlivých kódov prostredníctvom Sandbox technológie:	✓
Počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom:	min. 11000
Funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám:	✓
Možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS:	✓
Priepustnosť funkcie IPS vrátane logovania:	min. 2 Gbps
Funkcie antivírovej kontroly:	✓
Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom:	✓
AV kontrola rozšírená o inšpekciu tzv. sandbox technikou:	Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky
Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním:	min. 1,5 Gbps
Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hashov:	✓
Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky:	✓
Podpora SSL dešifrovania/SSL inšpekcie:	min. 1 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)
Funkcia DNS filtra:	✓
Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii:	✓
Možnosť definovať vlastný tzv. blacklist domén:	✓
Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL:	✓

Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos:	✓
Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri:	✓
Podpora SSL VPN:	✓
Priepustnosť SSL VPN:	min. 1 Gbps
Podpora IPSEC VPN v režime site-2-site aj client-2-site:	✓
Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B):	min. 11 Gbps
Podpora izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod.:	✓
FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu:	✓
Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky:	✓
Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete:	✓
Certifikácia ICSA Labs minimálne pre Firewall:	✓
Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať:	✓
Možnosť kombinovať akcie pre automatizačné pravidlá:	min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy.
Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel:	min. schopnosť parsovať vstupy z logov a z predchádzajúcich vykonaných akcií
Podpora otvoreného API pre ďalšie možnosti integrácie:	✓
Podpora SD-WAN:	✓
Podpora ZTNA:	✓
Podpora segmentácie sietí:	✓
Integrovaná konektivita switchov:	✓
Počet podporovaných switchov:	max. 32
Podpora vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie):	✓, v režime active-active (A/A) a active-passive (A/P); ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky
Prevedenie, výška:	rackové prevedenie, výška 1RU
Montážne príslušenstvo:	kompletné príslušenstvo (montážne prvky) pre montáž do racku;
Napájanie:	2x napájací redundantný napájací zdroj
Rozmery:	44 mm x 432 mm x 254 mm
Záručná doba a podpora:	3 roky, Hardware plus Premium and Enterprise Protection

02. Switch Layer 2/3, 24-port	*ks*			*2*

Technická špecifikácia:	Layer 2/3 switch od rovnakého výrobcu ako Firewall
Sloty:	min. 24 x GE/10GE SFP/SFP+ a min. 2 x 100GE QSFP28
Minimálna prepínacia kapacita (Duplex):	min. 880 Gbps
Minimálne spracovanie počtu paketov za sekundu:	min. 1300 Mpps
Latencia:	menej ako 1µs
Minimálny počet podporovaných VLAN:	4096
Minimálny počet agregačných skupín:	16
Podpora spájania zariadení do logického celku:	✓
Podpora Jumbo Frame:	✓
Podpora DHCP:	✓, DHCP Relay, DHCP snooping
Podpora RBAC:	✓
Podpora QoS 802.1p:	✓
Podpora 802.3ad Link Aggregation:	✓
Podpora 802.1q VLAN tagging:	✓
Podpora STP, RSTP, MSTP vrátane rozšírenia BPDU guard, Root guard, Loop guard:	✓
Zrkadlenie sieťových rozhraní (Port Mirroring):	✓
Podpora SNMP a syslog:	✓
Podpora IEEE 802.1X:	✓, Authentication Port-based, Authentication MAC-based, Guest and Fallback VLAN, Guest and Fallback VLAN, MAC Access Bypass (MAB), Dynamic VLAN Assignment, EAP pass-through,
Podpora Radius CoA (Change of Authority):	✓
Podpora Radius Accounting:	✓
Podpora MAC-IP Binding:	✓
Podpora sFlow:	✓
Podpora Flow Export - NetFlow v9 and IPFIX:	✓
Podpora ACL:	✓
Podpora IEEE 802.1ab:	✓, Link Layer Discovery Protocol (LLDP), LLDP-MED
Podpora IEEE 802.1ae:	✓, MAC Security (MAC Sec)
Podpora Dynamic ARP Inspection:	✓
Podpora IP source guard:	✓
Sticky MAC and MAC Limit:	✓
Per-port and per-VLAN MAC learning limit:	✓
Assign VLANs via Radius attributes (RFC 4675):	✓
CoS based (Ethernet) a CoS tag (802.1Q frames frames):	✓
IEEE 802.1p Based Priority Queuing:	✓
IP TOS/DSCP Based Priority Queuing:	✓
Explicit Congestion Notification:	✓
Egress priority tagging:	✓
DSCP-based a IP precedence CoS :	✓
QoS klasifikáci a markovanie na základe ACL (IP) - src/dst IP adresa, src/dst port, protocol:	✓
SSH a HTTPS management:	✓
Podpora REST API pre konfiguráciu a monitorovanie prvkov:	✓
Prepínače musia byť plne integrovateľné s centralizovanou platformou ako na funkčnej, tak na riadiacej úrovni:	✓

Plnou funkčnou integráciou je myslené minimálne:	✓
Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu:	✓
Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používateľa (firewally, prepínače, koncové stanice/užívatelia):	✓
Koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice:	✓
Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií:	✓
Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme:	✓
Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty):	✓, Možnosť konfigurácie časového intervalu tohto zobrazenia
Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo užívateľského mena:	✓
Možnosť hromadnej aktualizácie (upgrade) prepínačov z centrálnej konzoly:	✓
Podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača:	✓
Chladenie:	Smer prúdenia a odvod vzduchu spredu dozadu
Napájanie:	2x napájací redundantný napájací zdroj
Záručná doba a podpora:	3 roky, podpora typu Premium

03. Switch Layer 2, 48-port	*ks*			*9*
Technická špecifikácia:	management switch L2+ od rovnakého výrobcu ako Firewall			
Porty:	min. 48x GE port / min. 4x SFP+ port / min. 1x RJ45 konzolový port			
Minimálna prepínacia kapacita (Duplex):	min. 175 Gbps			
Minimálne spracovanie počtu paketov za sekundu:	min. 255 Mpps			
Latencia:	menej ako 1µs			
Mean Time Between Failures:	viacej ako 8 rokov			
Minimálny počet podporovaných VLAN:	min. 4096			
Počet agregačných skupín:	min. 12			
Podpora Auto-negotiation:	✓			
Podpora Jumbo Frame:	✓			
Podpora DHCP Relay:	✓			
Podpora DHCP snooping:	✓			
Podpora RBAC:	✓			

Podpora QoS 802.1p:	✓
Podpora 802.3ad Link Aggregation:	✓
Podpora 802.1q VLAN tagging:	✓
Podpora STP, RSTP, MSTP vrýtane rozšírenia BPDU guard, Root guard, Loop guard:	✓
Podpora IEEE 802.1ab LLDP-MED:	✓
Zrkadlenie sieťových rozhraní:	✓
Podpora Radius CoA (Change of Authority):	✓
Podpora 802.1x Radius:	✓
Podpora Radius Accounting:	✓
Podpora ACL:	✓
Podpora SNMP a syslog:	✓
SSH a HTTPS management:	✓
Podpora REST API pre konfiguráciu a monitorovanie prvkov:	✓
Prepínače musia byť plne integrovateľné s centralizovanou platformou ako na funkčnej, tak na riadiacej úrovni:	✓
Plnou funkčnou integráciou s centralizovanou platformou je myslené minimálne:	✓
Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu:	✓
Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používatela (firewally, prepínače, koncové stanice/užívatelia):	✓
Koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice:	✓
Možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno:	✓
Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií:	✓
Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme:	✓
Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia:	✓
Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom	✓

na základe MAC adresy, typu zariadenia, operačného systému alebo užívateľského mena:	
Možnosť hromadnej aktualizácie (upgrade) prepínačov z centrálnej konzoly:	✓
Podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača:	✓
Chladenie:	smer prúdenia a odvod vzduchu zo strany dozadu (side-to-back)
Záručná doba a podpora:	3 roky, podpora typu Premium

04. Switch Layer 2, 24-port	*ks*			*4*
Technická špecifikácia:	management switch L2 od rovnakého výrobcu ako Firewall			
Porty:	min. 24x GE port / min. 4x SFP+ port / min. 1x RJ45 konzolový port			
Minimálna prepínacia kapacita (Duplex):	min. 125 Gbps			
Minimálne spracovanie počtu paketov za sekundu:	min. 186 Mpps			
Latencia:	menej ako 1µs			
Mean Time Between Failures:	viacej ako 8 rokov			
Minimálny počet podporovaných VLAN:	min. 4096			
Počet agregačných skupín:	min. 12			
Podpora Auto-negotiation:	✓			
Podpora Jumbo Frame:	✓			
Podpora DHCP Relay:	✓			
Podpora DHCP snooping:	✓			
Podpora RBAC:	✓			
Podpora QoS 802.1p:	✓			
Podpora 802.3ad Link Aggregation:	✓			
Podpora 802.1q VLAN tagging:	✓			
Podpora STP, RSTP, MSTP vrátane rozšírenia BPDU guard, Root guard, Loop guard:	✓			
Podpora IEEE 802.1ab LLDP-MED:	✓			
Zrkadlenie sieťových rozhraní:	✓			
Podpora Radius CoA (Change of Authority):	✓			
Podpora 802.1x Radius:	✓			
Podpora Radius Accounting:	✓			
Podpora ACL:	✓			
Podpora SNMP a syslog:	✓			
SSH a HTTPS management:	✓			
Podpora REST API pre konfiguráciu a monitorovanie prvkov:	✓			
Prepínače musia byť plne integrovateľné s centralizovanou platformou ako na funkčnej, tak na riadiacej úrovni:	✓			
Plnou funkčnou integráciou s centralizovanou platformou je myslené minimálne:	✓			
Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu:	✓			
Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používatela (firewally, prepínače, koncové stanice/užívatelia):	✓			

Koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice:	✓
Možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno:	✓
Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií:	✓
Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme:	✓
Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia:	✓
Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo užívateľského mena:	✓
Možnosť hromadnej aktualizácie (upgrade) prepínačov z centrálnej konzoly:	✓
Podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača:	✓
Chladenie:	smer prúdenia a odvod vzduchu zo strany dozadu (side-to-back); bez ventilátorové
Záručná doba a podpora:	3 roky, podpora typu Premium

05. Switch Layer 2, 8-port	*ks* | | | *7*
Technická špecifikácia:	management switch L2 od rovnakého výrobcu ako Firewall
Porty:	min. 8x GE port / min. 2x GE SFP+ port
Minimálna prepínacia kapacita (Duplex):	min. 20 Gbps
Minimálne spracovanie počtu paketov za sekundu:	min. 28 Mpps
Latencia:	menej ako 4 µs
Mean Time Between Failures:	viacej ako 6 rokov
Minimálny počet podporovaných VLAN:	min. 4096
Počet agregačných skupín:	min. 4
Podpora Auto-negotiation:	✓
Podpora Jumbo Frame:	✓
Podpora DHCP Relay:	✓
Podpora DHCP snooping:	✓
Podpora RBAC:	✓
Podpora QoS 802.1p:	✓
Podpora 802.3ad Link Aggregation:	✓
Podpora 802.1q VLAN tagging:	✓

Podpora STP, RSTP, MSTP vrátane rozšírenia BPDU guard, Root guard, Loop guard:	✓
Podpora IEEE 802.1ab LLDP-MED:	✓
Zrkadlenie sieťových rozhraní:	✓
Podpora Radius CoA (Change of Authority):	✓
Podpora 802.1x Radius:	✓
Podpora Radius Accounting:	✓
Podpora ACL:	✓
Podpora SNMP a syslog:	✓
SSH a HTTPS management:	✓
Podpora REST API pre konfiguráciu a monitorovanie prvkov:	✓
Prepínače musia byť plne integrovateľné s centralizovanou platformou ako na funkčnej, tak na riadiacej úrovni:	✓
Plnou funkčnou integráciou s centralizovanou platformou je myslené minimálne:	✓
Jednotné riadiace (management) rozhranie, z ktorého je možné konfigurovať a riadiť ako prepínače tak aj firewall platformu:	✓
Vizualizácia logickej a fyzickej topológie celej infraštruktúry až do úrovne koncovej stanice/používateľa (firewally, prepínače, koncové stanice/užívatelia):	✓
Koncové zariadenia musia byť v jednotnom správcovskom (management) rozhraní graficky zobrazené s minimálne nasledujúcimi informáciami: názov zariadenia, typ a verzia OS, MAC adresy sieťových rozhraní, IP adresy, dátum posledného pripojenia do siete, počet otvorených spojení, množstvo prenesených dát, počet prenesených paketov, aktuálne využitá šírka pásma, užívateľské meno a detekované zraniteľnosti pracovnej stanice:	✓
Možnosť vyhľadávania konkrétnych zariadení alebo používateľov na základe minimálne nasledujúcich parametrov: IP adresa, MAC adresa, užívateľské meno:	✓
Vyhľadané zariadenie musí byť znázornené v rámci vizualizácie sieťovej topológie vrátane všetkých vyššie uvedených informácií:	✓
Možnosť manuálneho alebo automatického vloženia zariadení do karantény (samostatná VLAN/izolácia v rámci VLAN) na základe bezpečnostného incidentu detekovaného na firewall platforme:	✓
Vizualizácia množstva prenesených dát na jednotlivých portoch (access aj uplink porty). Možnosť konfigurácie časového intervalu tohto zobrazenia:	✓
Integrované natívne riešenie na kontrolu prístupu do siete (NAC funkcionalita) s možnosťou definície pravidiel minimálne pre automatické priraďovanie VLAN, QoS a 802.1X profilov jednotlivým portom na základe MAC adresy, typu zariadenia, operačného systému alebo užívateľského mena:	✓
Možnosť hromadnej aktualizácie (upgrade) prepínačov z centrálnej konzoly:	✓

Podpora spájania niekoľkých fyzických prepínačov do jedného logického prepínača:	✓
Chladenie:	smer prúdenia a odvod vzduchu zo strany dozadu (side-to-back); bez ventilátorové
Záručná doba a podpora	3 roky, podpora typu Premium

06. Modul 1GE SFP RJ45	*ks*			*15*
Technická špecifikácia:	1GE SFP RJ45 transceiver modul pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

07. Kábel 10GE passive direct attach cable SFP+ 1m	*ks*			*7*
Technická špecifikácia:	10 GE SFP+ passive direct attach cable (pasívny DAC), 1 m, pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

08. Kábel 10GE passive direct attach cable SFP+ 3m	*ks*			*8*
Technická špecifikácia:	10 GE SFP+ passive direct attach cable (pasívny DAC), 3 m, pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

09. Kábel 10GE passive direct attach cable SFP+ 5m	*ks*			*6*
Technická špecifikácia:	10 GE SFP+ passive direct attach cable (pasívny DAC), 5 m, pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

10. Optický modul 10GE SFP+RJ45, do 30 m	*ks*			*4*
Technická špecifikácia:	10 GE copper SFP+ RJ45 transceiver modul (vzdialenosť do 30 m) pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

11. Optický modul 10GE SFP+, do 300 m	*ks*			*4*
Technická špecifikácia:	10GE SFP+ transceiver modul, (vzdialenosť do 300 m) pre systémy s SFP a SFP/SFP+ slotmi, kompatibilný s obstarávanými zariadeniami			

12. SW monitorovanie a zhromažďovanie záznamov	*ks*			*1*
Technická špecifikácia:	Systém monitorovanie a zhromažďovanie logov			
Systém musí byť plne kompatibilný s dodávanými riešeniami:	NGFW/UTM, ZTNA, SWITCH			
Riešenie vo forme Virtual Appliance s podporou:	VMware, KVM alebo Hyper-V			
Schopnosť spracovávať logy v objeme GB/deň:	min. 1GB za deň			
Počet virtuálnych sieťových rozhraní:	min. 4			
Možnosť škálovateľného navýšenia objemu spracovávaných logov pomocou dodatočných licencií:	✓			
Možnosť škálovateľného navýšenia diskovej kapacity pomocou licencií:	✓			
Podpora SYSLOG, podpora šifrovaného prenosu dát/logov:	✓			
Riešenie musí obsahovať konfigurovateľné prehľady s drill down funkcionalitou:	✓			
Filtrovanie správ/logov na základe roznych parametrov, ich kombinácií. Podpora AND, OR logiky pri vytváraní filtrov:	✓			

Možnosť ukladania definícii filtrov pre rýchle opätovné použitie:	✓
Možnosť prehliadania logov v historickom alebo realtime režime:	✓
Možnosť zobrazovania logov v RAW alebo štruktúrovanom formáte:	✓
Korelácia logov:	✓
Možnosť automatického vytvárania incidentov:	✓
Možnosť automatického vyšetrovania incidentov pomocou definovateľných playbookov:	✓
Podpora Indication of Compromise - Systém musí obsahovať reputačné databázy nebezpečných IP/URL adries a musí vykonávať spätné prehľadávanie historických logov pri update reputačných DB za účelom detekcie napadnutia systémov a koncových staníc:	min. 5 dní do minulosti
Podpora vytvárania reportov:	min. vo formátoch PDF, HTML, CSV, XML
Možnosť generovania reportov v pravidelných intervaloch:	✓
Možnosť vytvárania vlastných požiadaviek voči databáze a ich použitie ako zdroj dát v reportoch:	✓
Podpora SNMP:	✓
Podpora REST API:	
GUI a CLI administračné rozhranie dostupné pomocou HTTPS a SSH protokolov:	✓
Podpora LDAP, RADIUS, Tacacs+ pre administrátorské účty:	✓
Záručná doba a podpora	3 roky, Premium Support (for 1-6 GB/Day of Logs)

13. SW klient pre vzdialené pripojenie – balík 25 ks	*ks*			*2*
Technická špecifikácia:	Klient na vzdialené pripojenie pre prenosné počítače pre 25 koncových bodov, od rovnakého výrobcu ako Firewall			
Podpora operačných systémov:	OS Windows, Linux, MacOS, Android, iOS			
Podpora Zero Trust Network Access (ZTNA):	✓			
Centrálna správa:	✓, Enterprise Management Server (EMS), riešenie pre bezpečnostnú centralizovanú správu viacerých koncových bodov (počítačov)			
Podpora cenrálneho logovania a reportovania:	✓			
Podpora viac faktorovej autentifikácie (MFA):	✓, pri SSL VPN a pri IPsec VPN			
Podpora Single Sign On Mobility Agent:	✓			
Podpora IT Hygiene Vulnerability Agent and Remediation:	✓			
Podpora Web Filtering:	✓			
Podpora Software Inventory:	✓			
Podpora Removable Media Control :	✓			
CASB Cloud/API-based CASB:	✓			
SaaS Application Control (Inline CASB):	✓			
Real-time SaaS Application Database Updates:	✓			
Malware Detection for Cloud Data:	✓			
IPsec VPN:	✓, podpora IKEv1 a IKEv2			
SSL VPN:	✓, podpora TLS 1.2 a TLS 1.3			

Podpora VPN Session AutoReconnect:	✓, s možnosťou neustáleho pripojenia do VPN a s možnosťou pripojenia do VPN pred prihlásením do operačného systému
Podpora Split Tunnel:	✓, na základe IP rozsahov, URL, FQDN, Aplikácií rozoznávaných na základe signatúr z Aplikačnej Kontroly
Možnosť povoliť/limitovať/zablokovať prístup do siete na základe stavu koncovej stanice:	✓
Riešenie musí umožňovať definíciu stavov koncovej stanice, a aplikovať takéto definície na základe pravidiel. Aktuálny stav koncových staníc musí byť možné vyčítavať pomocou REST API:	definícia stavov na základe: OS, Patch level, running process, registry key (windows), file, SSL certificate CN, a ich kombinácií
Riešenie musí umožniť aplikáciu konfigurácie z centrálneho managementu pre online klientov aj mimo internú sieť:	✓, synchronizácia konfigurácie medzi klientom a centrálnym managementom musí prebiehať automaticky, maximálna doba medzi synchronizáciami je 60 sekúnd
Riešenie musí poskytovať funkciu karantény pre koncové stanice:	✓
Podpora protokolu SAML SSO pre prihlasovanie do VPN (IPSEC, SSL):	✓
Podpora skenera zraniteľností:	✓, s možnosťou automatického aj manuálneho aplikovania bezpečnostných záplat. Možnosť periodických aj on-demand skenov
Podpora filtrácie prístupu na web na základe kategórií:	podpora min. 50 kategórií, možnosť nastavenia rôznych akcii povoliť/monitorovať/varovať/blokovať pre jednotlivé kategórie
Antimalware engine s možnosťou využívania cloudovej Sandbox služby:	✓
Antimalware engine založený na signatúrach a host-based Machine Learning:	✓
Antiexploit engine, systém musí byť schopný odhaliť známe metódy útokov, monitorovať správanie aplikácií (internetové prehliadače, JAVA, MS Office aplikácie, PDF prehliadače a pod.), chrániť koncové stanice pred memory based útokmi:	✓
Podpora Aplikačného firewallu s možnosťou povolenia alebo zablokovania aplikácií:	✓
Podpora monitoringu nainštalovaných aplikácií (Software inventár) vrátane zobrazenia verzii:	✓
Možnosť ukladať zablokované súbory do centrálnej karantény:	✓
Systém musí umožňovať detekciu či sa koncová stanica nachádza v internej alebo externej sieti a aplikovať rôzny profil pre rovnakého užívateľa a zariadenie na základe tejto detekcie:	✓
Centrálny management:	✓, musí obsahovať prehľadné a prispôsobiteľné dashboardy s informáciami o stave koncových staníc / musí obsahovať nástroje na diagnostiku problémov na koncových staniciach s min. možnosťou aktivácie debug módu a stiahnutie debug výstupov z koncovej stanice / musí umožňovať výber inštalácie On-prem alebo byť dostupný v cloud-e výrobcu
Záručná doba a podpora	3 roky, Premium Support (pre 1-6 GB/deň logov)

14. Etapa 2. poskytovanie profesionálnych služieb súvisiacich s dodávkou komponentov (aktívnych sieťových zariadení) na zvýšenie zabezpečenia siete a pre segmentáciu siete	*ks*			*1*
Technická špecifikácia:	Inštalácia, konfigurácia, nastavenia, migrácia, všetkých dodaných zariadení v sieti vrátane SW komponentov			

Etapa 2. poskytovanie profesionálnych služieb súvisiacich s dodávkou komponentov (aktívnych sieťových zariadení) na zvýšenie zabezpečenia siete a pre segmentáciu siete

Profesionálne služby súvisiace s dodávkou komponentov pre segmentáciu siete musia byť poskytované minimálne v nasledovnom obsahu:

- Detailná analýza potrieb zákazníckeho prostredia a následný návrh riešenia;
- Návrh musí byť spracovaný vo forme dokumentu, ktorý bude schválený objednávateľom.
- Realizácia riešenia je až po akceptácii návrhu architektúry
- Návrh musí spĺňať bezpečnostné štandardy v oblasti riadenia bezpečnosti sietí a informačných systémov pri zavádzaní súladu so ZoKB:
  - Segmentácia
  - Bezpečnostné politiky
  - Definovanie RBA -Role Based Access pre prístup na zariadenia
  - Implementáciu kontrolovaného prístupu pre koncových používateľov a zariadení
  - Definíciu bezpečnostných politík na prestup medzi jednotlivými segmentami infraštruktúry
  - Implementácia všetkých best practice
- V rámci ponuky musí byť fyzická inštalácia zariadení;
- V rámci ponuky je požadovaná konfigurácia zariadení a jednotlivých komponentov;
- V rámci ponuky je požiadavka na migráciu komponentov existujúceho prostredia;
- V rámci ponuky je požiadavka na integráciu s komponentami existujúceho prostredia;
- V rámci akceptácie implantácie sú požadované SAT – Site Acceptance Tests;
- V rámci akceptácie implantácie sú požadované FAT – Factory Acceptance Tests;
- V rámci ponuky je požadované spustenie komponentov infraštruktúry do produkčnej prevádzky;
- Zaškolenie interných zamestnancov.

Termín dodávky

Dodávka Etapy 1: (zariadení a príslušenstva) maximálne do 42 kalendárnych dní od účinnosti zmluvy.
Dodávka Etapy 2: (profesionálnych služieb) maximálne do 30 kalendárnych dní od ukončenia Etapy 1