Smlouva na dodávku prvků pro řízený a bezpečný přístup do vnitřní sítě

uzavřená podle § 1746, odst. 2 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „smlouva“), ev. č.: ANECT/MUH-1/2020/003, v návaznosti na veřejnou zakázku malého rozsahu uveřejněnou kupujícím jako veřejným zadavatelem mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek, pod názvem „Prvky pro řízený a bezpečný přístup do vnitřní sítě“ (dále jen „veřejná zakázka“). Nabídka prodávajícího na plnění veřejné zakázky byla kupujícím vyhodnocena jako nejvýhodnější.

Článek 1: Smluvní strany

Objednatel: **Město Uherské Hradiště**

sídlo: Masarykovo náměstí 19, 686 01 Uherské Hradiště

zastoupena: Ing. Stanislavem Blahou, starostou města

IČ: 00291471

DIČ: CZ00291471

Osoba oprávněná k převzetí věci: Mgr. Jiří Dorogy, odbor organizační správy a informatiky, tel.: 572 525 144, jiri.dorogy@mesto-uh.cz.

(dále v této smlouvě označován jen jako „Objednatel“)

Dodavatel: **ANECT a.s.**

sídlo: Vídeňská 204/125, Přízřenice, 619 00 Brno

kterou zastupuje: Jan Zinek, předseda představenstva

IČ: 25313029

DIČ: CZ25313029

zapsaná u rejstříkového soudu v Brně pod sp. zn. B 2113

Bankovní spojení: Komerční banka, a.s., č. účtu: 27-6667590237 / 0100

(dále v této smlouvě označován jen jako „Dodavatel“)

(společně také jako „Smluvní strany“)

Článek 2: Předmět smlouvy

1. Dodavatel se zavazuje zajistit Objednateli dodání a instalaci, implementaci a servisní podporu kombinovaného řešení s těmito funkcemi: Perimetrový next-gen Firewall fungující v režimu vysoké dostupnosti s centralizovaným managementem a Přístupový bod do vnitřní sítě pomocí klientské VPN pro 50 klientů s možností dalšího rozšíření na minimálně 130 klientů. Součástí dodávky je podpora výrobce, všechny potřebné licence a SW/HW podpora na období 5 let (dále jen „Plnění). Bližší specifikace Plnění je uvedena v Příloze č. 1 této smlouvy, která odpovídá příloze č. 2 zadávací dokumentace k veřejné zakázce.
2. Objednatel se zavazuje umožnit Dodavateli poskytnout Plnění a zaplatit za něj dohodnutou cenu.

Článek 3: Doba a místo Plnění

1. Dodavatel zahájí poskytování Plnění bezprostředně po podpisu smlouvy a dokončí poskytování Plnění do 31.12.2020. Dále Dodavatel zajistí Objednateli poskytování odborné podpory výrobce po dobu 5 let od data předání dodávaného řešení Objednateli.
2. Dodavatel bude Objednateli poskytovat Plnění v sídle Objednatele na adrese budova Městského úřadu Uherské Hradiště, Masarykovo náměstí 19, Uherské Hradiště.

Článek 4: Cena a platební podmínky

1. Cena Plnění je stanovena dohodou obou smluvních stran jako nejvýše přípustná na částku: **327 722,55 Kč** (slovy: tři sta dvacet sedm tisíc sedm set dvacet dva korun českých padesát pět haléřů) bez DPH, tj. **396 544,29 Kč** (slovy: tři sta devadesát šest tisíc pět set čtyřicet čtyři korun českých dvacet devět haléřů) včetně DPH.
2. Cena Plnění bude zaplacena dopředu jednorázovou platbou na účet Dodavatele.
3. Datem uskutečnění zdanitelného plnění ve vztahu upraveném touto smlouvou je datum vzájemně odsouhlaseného a podepsaného předávacího protokolu.
4. Splatnost daňového dokladu (faktury) za dodané plnění je splatná 30 dní od jejího doručení Objednateli. Faktura bude zaslána Objednateli elektronicky.

Článek 5: Garance a sankce

1. Smluvní strany se dohodly na následujících sankcích za porušení svých povinností dle smlouvy:

Sankce	Hodnota
Sankce vůči Dodavateli za nedodržení dohodnutých smluvních podmínek termínu dodání předmětu smlouvy v % / den s DPH	0,04
Sankce vůči Objednateli za nedodržení termínu splatnosti faktur v %/den	0,04
Sankce vůči Dodavateli za nedodržení SW/HW podpory (next business day)	1.000 Kč/den

Článek 6: Trvání a ukončení smlouvy

2. Smlouva se uzavírá na dobu určitou do doby poskytování odborné podpory výrobce na dodaný produkt.
3. Smluvní vztah lze ukončit kdykoliv vzájemnou dohodou smluvních stran.

Článek 7: Závěrečná ustanovení

1. Zástupci obou smluvních stran výslovně prohlašují, že jsou zcela oprávněni uzavřít tuto smlouvu.
2. Smlouva nabývá platnosti dnem podpisu smluvními stranami a účinnosti dnem uveřejněním v registru smluv.
3. Tato smlouva může být doplňována či měněna pouze písemnými dodatky podepsanými oprávněnými zástupci obou smluvních stran. Dodatky budou chronologicky seřazeny v časovém sledu a číslovány.
4. Stanou-li se některá ustanovení této Smlouvy zcela nebo zčásti neplatná, nebo pokud by některá ustanovení chyběla, není tím dotčena platnost zbývajících ustanovení. Místo neplatného ustanovení platí jako dohodnuté takové ustanovení, které odpovídá smyslu a účelu neplatného ustanovení. Schází-li ustanovení zcela, platí za dohodnuté takové ustanovení, které odpovídá tomu, co by podle smyslu a účelu této Smlouvy bylo ujednáno, kdyby tato skutečnost byla známa od počátku.
5. Dodavatel se zavazuje, že v případě nabytí statutu „nespolehlivý plátce“, ve smyslu zákona

č. 235/2004 Sb. o dani z přidané hodnoty, bude o této skutečnosti neprodleně objednatele informovat. Objednatel je poté oprávněn zaslat hodnotu plnění odpovídající dani z přidané hodnoty přímo na účet správce daně v režimu podle § 109a výše uvedeného zákona.

6. Dodavatel bere na vědomí, že tato smlouva a případně i její budoucí dodatky mohou být Objednatelem uveřejněny ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění (dále jen „zákon o registru smluv“), neboť Objednatel je mj. povinným subjektem dle citovaného zákona. Pro tyto případy je Dodavatel povinen Objednatele písemně upozornit na případné obchodní tajemství a jiné chráněné údaje vyplývající z této smlouvy, případně i jejich budoucích dodatků, které budou následně Objednatele v uveřejňovaném textu anonymizovány.
7. Nedílnou součástí této smlouvy je Příloha č. 1.
8. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá strana obdrží po jednom vyhotovení.
9. Smlouva je ukončena uplynutím doby, na kterou byla uzavřena.
10. Doložka podle ustanovení § 41 zákona o obcích: O uzavření této smlouvy bylo rozhodnuto usnesením Rady města Uherské Hradiště č. 773/53/RM/2020 ze dne02.12.2020.

V Uherském Hradišti dne:	V Praze dne:
Za Objednatele:	Za Dodavatele:
……..	……..
Ing. Stanislav Blaha,	Jan Zinek
starosta města	předseda představenstva

Příloha č. 1

Prvky pro řízený a bezpečný přístup do vnitřní sítě (minimální parametry)

Požadovaná funkcionalita / vlastnost	Nabízené řešení splňuje / nesplňuje požadavek kupujícího (doplní uchazeč ANO / NE)		Hodnota nabízeného technického parametru nebo způsob zabezpečení technického požadavku
Firewall (FW)- 2 ks zařízení v režimu vysoké dostupnosti včetně pětileté podpory výrobce			
Cisco Firepower FPR1120-FTD			
Výkonové paramentry a funkce FW na perimetru			
Formát zařízení	Appliance, 1RU	ANO	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	ANO	1
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro data, standardně osazených	12	ANO	12
Minimální počet SFP slotů, standardně osazených	4	ANO	4
Osazeno USB rozhraním pro lokální práci se soubory	Ano	Ano	1 x USB 3.0 Type-A (500mA)
Podporovaný počet současně otevřených spojení aplikační FW	200K	ANO	200.000
Rychlost vytváření nových spojení přes aplikační FW	12K/s	ANO	15.000/s
Propustnost aplikačního FW (next-gen FW)	1,25 Gbps	ANO	1,5 Gbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS)	1,25 Gbps	ANO	1,5 Gbps
Minimální počet VPN peerů	130	ANO	150
Propustnost IPSec VPN	900 Mbps	ANO	1000 Mbps
Podpora L2 (bridging) módu s podporou NAT a PAT	Ano	ANO	
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO	
Podpora IPS inline (plně transparentního) módu	Ano	ANO	
Podpora 802.1Q tagovaných rámců	Ano	ANO	
Podporovaný počet VLAN	Min. 1024	ANO	1 - 4094
Podpora stateful failover	active/standby	ANO	active/standby
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO	
Dynamické směrování - podpora minimálně RIP, OSPF, BGP	Ano	ANO	
Podpora IPv6 dynamického směrování – minimálně OSPFv3, BGP	Ano	ANO	
Podpora Policy based Routing	Ano	ANO	
Podpora virtuálních směrovacích instancí (VRF)	Ano	ANO	
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO	
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	ANO	
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano	ANO	
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	ANO	

Funkce Next-Gen FW			
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO	
Podpora pasivního monitorování (TAP režim)	Ano	ANO	
Podporovaných aplikací	Min. 3000	ANO	4000+
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO	
URL kategorie	80	ANO	80+
Katagorizovaných světových URL	280 milionů	ANO	280.000.000+
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano	ANO	
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO	
Filtrace podle reputace serverů	Ano	ANO	
SSL inspekce (dekrypce/enkrypce)	Ano	ANO	
Hardwarová akcelerace TLS	Ano	ANO	
Security Inteligence database – známé uzly botnet sítí C&C	Ano	ANO	
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	ANO	
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	Ano	ANO	
Možnost integrovat vlastní reputační databáze	Ano	ANO	
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO	

Podpora filtrování provozu			
Podpora filtrace IPv4, IPv6	Ano	ANO	
Podpora filtrace podle bezpečnostních zón	Ano	ANO	
Podpora filtrace podle VLAN tagů	Ano	ANO	
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO	
Podpora filtrace podle aplikace, kategorie rizikovosti a business relevance	Ano	ANO	
Podpora filtrace podle bezpečnostních skupin naučených z RADIUS serveru	Ano	ANO	
Podpora filtrace podle atributů získaných přes pxGrid z ISE (např. typ platformy)	Ano	ANO	
Podpora konfigurace logování per přístupové pravidlo	Ano	ANO	
Podpora aplikace IPS politik per přístupové pravidlo	Ano	ANO	

Funkce Intrusion Prevention Systém			
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO	
Podpora IDS režimu – pasivního monitorování (TAP režim)	Ano	ANO	
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	ANO	
Podpora různých IPS politik pro různé typy provozu	Ano	ANO	
Inspekce pro IPv4 i IPv6	Ano	ANO	
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano	ANO	

Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	ANO	
Podpora importu komunitních filtrů/signatur Snort	Ano	ANO	
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO	
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	ANO	
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano	ANO	
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano	ANO	
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	ANO	
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano	ANO	
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	ANO	
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	ANO	
Možnost definice uživatelské vrstvy politik	Ano	ANO	
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	ANO	
Automatická klasifikace nebezpečnosti útoku relevantní ke konkrétnímu prostředí	Ano	ANO	
Interní korelaci bezpečnostních incidentů na endpointech s propagací do zobrazení kompromitovaných stanic	Ano	ANO	
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	ANO	
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	ANO	
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	ANO	
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	ANO	
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	ANO	

Možnosti integrace a další funkcionality FW			
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	ANO	
Funkce omezování datové rychlosti (rate limit) až do úrovně jednotlivých toků (flow) definovaných v přístupových pravidlech	Ano	ANO	
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO	

Podpora NAT64 a DNS64	Ano	ANO	
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO	
Podpora export informací o spojeních do netflow kolektoru	Ano	ANO	
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení a musí poskytovat minimálně tyto informace: Typ zařízení, Operační systém, Dodavatel OS, Použité síťové protokoly, Použité síťové služby, Otevřené porty síťových služeb a Potenciální zranitelnosti	Ano	ANO	
Přehled o síťových spojeních musí poskytovat minimálně tyto informace: Čas startu a konce flow, Akce (allow, deny,..), Důvod případného blokování, Zdrojovou a cílovou adresu, Vstupní a výstupní zónu, Vstupní a výstupní rozhraní, Zdrojový a cílový port, Aplikační protokol, IPS událost (pokud vznikne), Rizikovou úroveň IPS události, Použitou síťovou aplikaci, Rizikovost aplikace, "Business impact" aplikace a Množství přenesených dat	Ano	ANO	
Možnost integrace externích systémů (např. detektoru zranitelností Qualys) s propagací zranitelnosti do automatického nastavení IPS	Ano	ANO	
Funkcionalita VPN			
Podpora IPSec VPN	Ano	ANO	
IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol	Ano	ANO	
Podpora nového protokolu pro výměny klíčů IKEv2	Ano	ANO	
Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256	Ano	ANO	
Podpora kontrolních mechanizmů: MD5, SHA	Ano	ANO	
Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256	Ano	ANO	
Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384	Ano	ANO	
Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA	Ano	ANO	
Podpora klientské SSL VPN	Ano	ANO	
Podpora TLS 1.2 pro SSL VPN	Ano	ANO	
Podpora DTLS pro SSL VPN	Ano	ANO	
Minimální kapacita platformy pro konkurentní SSL VPN připojení	130	ANO	150
Možnost autorizovat přístup k SSL VPN Radius serverem	Ano	ANO	
Možnost ovlivnit politiku připojení k SSL VPN na úrovni jednotlivých klientů	Ano	ANO	
Možnost filtrovat provoz od SSL VPN klientů přímo na zařízení	Ano	ANO	
Identita SSL VPN klientů ověřitelná přes Radius server	Ano	ANO	
Identita SSL VPN klientů ověřitelná přes Microsoft AD nebo LDAP	Ano	ANO	
Ověření SSL VPN klientů přes multi faktorovou autentizaci Cisco DUO	Ano	ANO	

Podpora ověření VPN klientů certifikátem	Ano	ANO	
Možnost mapování nějakého CN certifikátu na přístupová pravidla	Ano	ANO	
Využití CN v certifikátu pro autorizaci ve spojení s RADIUS/AD/LDAP	Ano	ANO	
Podpora split i non-split klientské VPN	Ano	ANO	
Možnost centrálního ověření zdraví koncové stanice před připojením do klientské VPN (aktuální OS, aktuální antivirová databáze apod.) pomocí ISE	Ano	ANO	
Možnost integrace MFA s detekcí zdraví koncové stanice	Ano	ANO	

Centrální management Firewallu			
Cisco Firepower Management Center			
Funkcionality Centrálního managementu			
Virtual appliance	Ano	ANO	VMware, KVM
Minimální počet spravovaných sensorů/FW	2	ANO	2
Minimální kapacita IPS eventů	10M	ANO	10.000.000
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	ANO	
Přístup ke GUI http/https protokolem	Ano	ANO	
Možnost centrální správy při nasazení více firewallů	Ano	ANO	
Možnost sdílených bezpečnostních politik	Ano	ANO	
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	ANO	
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	ANO	
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	ANO	
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap	Ano	ANO	
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod.	Ano	ANO	
Centrální management musí být schopný dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	ANO	
Centrální management musí být schopný poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	ANO	
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI Centrálního managementu	Ano	ANO	
Přehledy a statistiky v Centrálním managementu lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	ANO	
Centrální management musí být schopný vytvářet reporty manuálně a podle časového harmonogramu	Ano	ANO	
Pro reporty lze definovat template definující formát a obsah reportu	Ano	ANO	
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	ANO	
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	ANO	

Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	ANO	
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	ANO	
Centrální management musí být schopný integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	ANO	
Centrální management musí být schopný integrace s Cisco ISE pomocí protokolu pxGrid pro získání aktuálních dat o zařízeních připojených do sítě.	Ano	ANO	
Centrální management musí být schopný ve spojení s Cisco ISE uvést koncové zařízení do rychlé karantény při detekci závadného provozu.	Ano	ANO	
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	ANO	
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	ANO	
Podpora Event Streamer API (eStreamer) pro sdílení informací s externími systémy - minimálně pro tyto SIEM: ArcSight, Novell Sentinel, Q1Labs-QRadar, Log Rhythm SIEM 2.0, LogLogic a Splunk	Ano	ANO	
Podpora integrace s autentizačním RADIUS serverem pomocí zabezpečeného protokolu SSL/TLS	Ano	ANO	
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	ANO	
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	ANO	
Podpora řízeného přístupu podle rolí administrátorů	Ano	ANO	
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	ANO	
Možnost definovat domény a k nim přidělit spravovaná zařízení pro oddělení správy a monitoringu podle RBAC	Ano	ANO	
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a Centrálním managementu (zařížení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	ANO	
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	ANO	
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory/firewally nebo Centrální management	Ano	ANO	
API pro možnost integrace do centrální platformy monitorování, diagnostiky a automatizace firemní bezpečnosti	Ano	ANO	

Vysvětlivky:

Uchazeč vyplní pouze žlutě podbarvené buňky, obsah a vzorce ostatních buněk nesmí upravovat.

Hodnota uvedená ve sloupci B je minimální, musí ji nabízené zařízení splňovat.