

Príloha č. 1 súťažných podkladov

Názov predmetu zákazky:

Technológie sieťovej a komunikačnej bezpečnosti**IDENTIFIKAČNÉ ÚDAJE UCHÁDZAČA**

Obchodné meno/názov uchádzača:	SmartSec Technologies s.r.o.
Sídlo alebo miesto podnikania :	Jégeho 6, Bratislava 821 08
IČO:	50448676
DIČ:	2120361452
IČ DPH:	SK2120361452
Právna forma :	s.r.o.
URL :	www.smartsectechnologies.sk
Zápis uchádzača v Obchodnom registri (označenie Obchodného registra alebo inej evidencie, do ktorej je uchádzač zapísaný podľa právneho poriadku štátu, ktorým sa spravuje, a číslo zápisu alebo údaj o zápise do tohto registra alebo evidencie):	
Zoznam osôb oprávnených konať v mene uchádzača :	Ing. Jozef Dbiš, konateľ
Zápis uchádzača v Zozname hospodárskych subjektov (uchádzač uvedie registračné číslo zápisu do ZHS) :	2024/12-PO-G9515
Zápis uchádzača v Registri partnerov verejného sektora (uchádzač uvedie číslo vložky zápisu do RPVS):	12995
Uchádzač je MSP : MSP je skratka mikro, malých a stredných podnikov (Mikropodniky: podniky, ktoré zamestnávajú menej ako 10 osôb a ktorých ročný obrat a/alebo celková ročná súvaha neprekračuje 2 milióny EUR Malé podniky: podniky, ktoré zamestnávajú menej ako 50 osôb a ktorých ročný obrat a/alebo celková ročná súvaha neprekračuje 10 miliónov EUR Stredné podniky: podniky, ktoré nie sú mikropodnikmi ani malými podnikmi a ktoré zamestnávajú menej ako 250 osôb a ktorých ročný obrat neprekračuje 50 miliónov EUR a/alebo celková ročná súvaha neprekračuje 43 miliónov EUR)	MSP

Kontaktná osoba uchádzača - počas procesu VO

Meno a priezvisko:	Jozef Dobiš
Telefónne číslo:	
E-mail:	jd@smartsectechnologies.sk

Údaje o osobe podľa § 49 ods. 5 ZVO

Meno a priezvisko:	
Obchodné meno/názov:	
Adresa pobytu/Sídlo alebo miesto podnikania:	
IČO:	

(vyplní uchádzač , ak je to relevantné)

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby Jozef Dobiš

podpis a pečiatka uchádzača

Názov predmetu zákazky:

Technológie sieťovej a komunikačnej bezpečnosti

ČESTNÉ VYHLÁSENIE UCHÁDZAČA VO VEREJNOM OBSTARÁVANÍ

Obchodný názov uchádzača: **SmartSec Technologies s.r.o.**

Sídlo alebo miesto podnikania: Jégeho 6, Bratislava 821 08

IČO: 50448676

DIČ: 2120361452

IČ DPH: SK2120361452

Ako štatutárny orgán vyššie uvedeného uchádzača týmto čestne vyhlasujem, že ako uchádzač vo verejnom obstarávaní na uvedený predmet zákazky:

- bezvýhradne súhlasím a plne akceptujem ustanovenia návrhu zmluvy a bezvýhradne súhlasím s podmienkami uvedenými v Oznámení o vyhlásení verejného obstarávania, v týchto súťažných podkladoch a v ostatných dokumentoch poskytnutých verejným obstarávateľom,
- všetky predložené doklady, dokumenty, vyhlásenia a údaje uvedené v ponuke a predložené s ponukou sú pravdivé a úplné,
- všetky doklady, dokumenty a vyhlásenia predložené v ponuke, ktoré neboli pôvodne vyhotovené v elektronickej podobe sú zhodné s originálnym vyhotovením, ktoré máme ako uchádzač k dispozícii v listinnej podobe
- nie sme členom skupiny dodávateľov, ktorá predkladá ponuku v súlade s ustanovením § 49 ods. 6 zákona o verejnom obstarávaní
- som zapísaný v Registri partnerov verejného sektora . Povinnosť zápisu do registra partnerov verejného sektora upravuje osobitný predpis – zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov
- dávam písomný súhlas k tomu, aby kópia našej ponuky bola zverejnená v Profile verejného obstarávateľa v súlade s § 64 ods. 1 písm. b) zákona o verejnom obstarávaní;

naša spoločnosť nie je čo i len v potenciálnom konflikte záujmov vo vzťahu k verejnému obstarávateľovi, jeho zamestnancom alebo vo vzťahu k osobám, ktoré sa podieľali na príprave a realizácii verejného obstarávania; nevyvíjali a nebudeme vyvíjať voči žiadnej osobe na strane verejného obstarávateľa ktorá je alebo by mohla byť zainteresovaná v zmysle ustanovení § 23 ods. 3 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších

- predpisov („zainteresovaná osoba“) akékoľvek aktivity, ktoré vy mohli viesť k zvýhodneniu nášho postavenia vo verejnom obstarávaní; neposkytli a neposkytneme akékoľvek, čo i len potenciálne zainteresovanej osobe priamo alebo nepriamo akúkoľvek finančnú alebo vecnú výhodu ako motiváciu alebo odmenu súvisiacu s týmto verejným obstarávaním a budeme bezodkladne informovať verejného obstarávateľa o akékoľvek situácii, ktorá je považovaná za konflikt záujmov alebo ktorá by mohla viesť ku konfliktu záujmov kedykoľvek v priebehu procesu verejného obstarávania.

oboznámil som sa s etickým kódexom záujemcu/uchádzača vo verejnom obstarávaní, ktorý je zverejnený na adrese <https://www.uvo.gov.sk/extdoc/13427> a v nadväznosti na uvedené vyhlasujem, so zreteľom na povinnosť uplatňovania

- princípov rovnakého zaobchádzania, nediskriminácie, transparentnosti, hospodárnosti a efektívnosti, zabezpečovania čestnej hospodárskej súťaže, vykonávania práv a povinností v súlade s dobrými mravmi a so zásadami poctivého obchodného styku, že budem tieto pravidlá aplikovať v rámci daného postupu verejného obstarávania.

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby
podpis a pečiatka uchádzača

Jozef Dobiš

Názov predmetu zákazky:

Technológie sieťovej a komunikačnej bezpečnosti

**ČESTNÉ VYHLÁSENIE UCHÁDZAČA
O NEULOŽENÍ ZÁKAZU ÚČASTI VO VEREJNOM OBSTARÁVANÍ**

Obchodný názov uchádzača: **SmartSec Technologies s.r.o.**

Sídlo uchádzača: Jégeho 6, Bratislava 821 08

IČO: 50448676

DIČ: 2120361452

IČ DPH: SK2120361452

Týmto vyhlasujem, že:

- nemám uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v Slovenskej republike a v štáte sídla, miesta podnikania alebo obvyklého pobytu.

Zároveň prehlasujem, že som si vedomý následkov nepravdivého čestného vyhlásenia.

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby
podpis a pečiatka uchádzača

Jozef Dobiš

Technológie sieťovej a komunikačnej bezpečnosti

**ČESTNÉ VYHLÁSENIE UCHÁDZAČA
K UPLATŇOVANIU MEDZINÁRODNÝCH SANKCIÍ**

Obchodný názov uchádzača: **SmartSec Technologies s.r.o.**
Sídlo uchádzača: Jégeho 6, Bratislava 821 08
IČO: 50448676
DIČ: 2120361452
IČ DPH: SK2120361452

Týmto čestne vyhlasujem(e), že:

v spoločnosti, ktorú zastupujem a ktorá podáva ponuku do predmetného verejného obstarávania a ktorá bude zároveň vykonávať plnenie zákazky, nefiguruje ruská účasť, ktorá prekračuje limity stanovené v článku 5k nariadenia Rady (EÚ) č. 833/2014 z 31. júla 2014 o reštriktívnych opatreniach s ohľadom na konanie Ruska, ktorým destabilizuje situáciu na Ukrajine v znení nariadenia Rady (EÚ) č. 2022/578 z 8. apríla 2022.

Predovšetkým vyhlasujem(e), že:

- (a) dodávateľ, ktorého zastupujem (a žiadna zo spoločností, ktoré sú členmi nášho konzorcia), nie je ruským štátnym príslušníkom ani fyzickou alebo právnickou osobou, subjektom alebo orgánom so sídlom v Rusku;
- (b) dodávateľ, ktorého zastupujem (a žiadna zo spoločností, ktoré sú členmi nášho konzorcia), nie je právnickou osobou, subjektom alebo orgánom, ktorých vlastnícke práva priamo alebo nepriamo vlastní z viac ako 50 % subjekt uvedený v písmene a) tohto odseku;
- (c) ani ja, ani spoločnosť, ktorú zastupujeme, nie sme fyzická alebo právnická osoba, subjekt alebo orgán, ktorý koná v mene alebo na príkaz subjektu uvedeného v písmene a) alebo b) uvedených vyššie;
- (d) subdodávatelia, dodávatelia alebo subjekty, na ktorých kapacity sa dodávateľ, ktorého zastupujem spolieha, subjektami uvedenými v písmenách a) až c), nemajú účasť vyššiu ako 10 % hodnoty zákazky.

Zároveň čestne vyhlasujem, že táto ponuka/žiadosť o účasť a realizácia plnenia podľa zmluvy, ktorá bude výsledkom daného verejného obstarávania zo strany hospodárskeho subjektu, ktorý zastupujem, nie je v rozpore so zákonom č. 289/2016 Z. z. o vykonávaní medzinárodných sankcií v znení neskorších predpisov, a teda najmä neporušuje akúkoľvek medzinárodnú sankciu upravenú v akomkoľvek predpise o medzinárodnej sankcii podľa § 2 písm. b) zákona č. 289/2016 Z. z. o vykonávaní medzinárodných sankcií v znení neskorších predpisov.

Súčasne prehlasujem, že som si vedomý následkov nepravdivého čestného vyhlásenia.

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby
podpis a pečiatka

Jozef Dobiš

Uchádzač (obchodné meno):	SmartSec Technologies s.r.o.
Sídlo:	Jégeho 6, Bratislava 821 08
IČO:	50448676
DIČ:	2120361452
IČ DPH:	SK2120361452

ŠPECIFIKÁCIA PREDMETU ZÁKAZKY

1.1 Názov predmetu zákazky:

Technológie sieťovej a komunikačnej bezpečnosti pre projekt "Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti"

1.2 CPV:

32420000-3 Sieťové zariadenia

1.3 Druh:

tovar, služba

1.4 Položky predmetu zákazky

Zoznam položiek:

Poradové číslo	Názov položky predmetu zákazky	MJ	Požadovaný počet MJ za zmluvné obdobie
Položka č. 1	Firewall	ks	2
Položka č. 2	Služby spojené s dodávkou Firewall	ks	1

TECHNICKÁ ŠPECIFIKÁCIA PREDMETU ZÁKAZKY

Požadované minimálne technické vlastnosti, parametre a hodnoty predmetu zákazky					Uchádzač uvedie informácie, či ním ponúkaný produkt spĺňa, resp. nesplňa verejným obstarávateľom definované požiadavky na predmet zákazky a uvedie aj hodnoty parametrov (v prípade, ak ponúkaný produkt nesplňa definované požiadavky uvedie ekvivalentnú hodnotu ním ponúkaného produktu)	
					spĺňa / nesplňa	hodnota ponúkaného ekvivalentného produktu
Položka č. 1 Firewall (minimálne požiadavky na každý jeden kus)					parametre	
					MJ	min.
					max.	presne
Základné požiadavky:	Bezpečnostné zariadenie typu next-generation firewall (ďalej tiež len NGFW) musí byť ako celok zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod.. Zároveň musí byť týmto jedným výrobcom zaistená podpora minimálne počas plánovanej životnosti NGFW					
					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series

	Výrobca NGFW sa musí nachádzať v "Leaders" kvadrante Enterprise Network Firewalls v poslednom aktuálnom reporte spoločnosti Gartner					spĺňa	https://www.paloaltonetworks.com/blog/2025/08/hybrid-mesh-firewall-magicquadrant/
Požiadavky na HW architektúru:	Všetky parametre priepustnosti musí dodávateľ uvádzať v real world mix paketoch, tzv. "application mix"					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	Modul na spracovanie dát musí byť v architektúre firewallu oddelený minimálne na úrovni CPU jadier od ďalších podporných modulov (správa zariadení a riadiaci modul pre podporné sieťové činnosti), aby nemohlo dôjsť k ich vzájomnému ovplyvneniu					spĺňa	Dokument detailne popisuje ako je možné dedikovať CPU pre data a management plane: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/virtualization-features/customize-dataplane-cores
	Konkrétny text: ..the memory profile and the total number of vCPUs determine how many cores are automatically assigned to the management plane and the dataplane. The default configurations perform well in most cases.						
	NGFW musí obsahovať min. jeden dedikovaný port pre správu pomocou konzoly pre prístup k CLI					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí obsahovať minimálne 10 ks optických dátových rozhraní SFP+ s rýchlosťou 10 Gb/s	ks	10			spĺňa / 10 ks	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)						
	NGFW musí obsahovať minimálne 4 ks optických dátových rozhraní SFP28 rozhraní s rýchlosťou 25 Gb/s	ks	4			spĺňa / 4 ks	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)						
	NGFW musí obsahovať minimálne jeden dedikovaný OOB manažment port pre plnohodnotnú správu NGFW					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí byť schopný ukladať logové údaje na interný storage o veľkosti minimálne 460 GB	GB	460			spĺňa / 480 GB	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: 480 GB SSD						
	NGFW musí podporovať agregáciu portov pomocou protokolu 802.3ad (LACP)					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series

	NGFW musí byť rozmerovo kompatibilný s 19" rozvádzačom					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať dva nezávislé redundantné zdroje napájania AC 230V, vymeniteľné za behu zariadenia					spĺňa	https://docs.paloaltonetworks.com/hardware/pa-3400-hardware-reference/service-pa-3400-seriesfirewall/replace-power-supply-pa-3400-series
Požiadavky na High Availability (HA):	NGFW musí podporovať režim HA v móde Active-Active zložený min. z dvoch zariadení					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať režim HA v móde Active-Standby zložený min. z dvoch zariadení					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/high-availability/set-upactivepassive-ha/configure-activepassive-ha
	NGFW musí podporovať rozšírenie výkonu a kapacity zariadenia (HA clusteru) len pridaním ďalšieho zariadenia za pomoci externého load balancera.					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/high-availability/haclustering-overview
	NGFW musí podporovať režim klasteringu, využiteľný pre prípadné dodatočné zvýšenie priepustnosti aj v geograficky oddelených lokalitách					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/high-availability/haclustering-overview
	V oboch typoch HA musia byť všetky informácie o prebiehajúcej prevádzke synchronizované tak, aby pri výpadku jedného z boxov nedošlo k strate informácií NAT ak prerušeniu aktívnych spojení prevádzky typu TCP i UDP prechádzajúceho cez NGFW					spĺňa	https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Ciy1CAK
	NGFW musí byť schopný vykonať HA failover na základe stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti špecifikovanej IP adresy					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/high-availability
Všeobecné výkonové parametre:	Priepustnosť firewallu pri plnej aplikačnej kontrole musí dosahovať hodnoty min. 13,9 Gb/s (app mix)	Gb/s	13,9			spĺňa / 14 Gbps	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: Firewall throughput (appmix)* 14 Gbps						
	Priepustnosť firewallu pri plnej aplikačnej kontrole a zapnutí všetkých dostupných signatúr IPS a AV musí dosahovať hodnoty min. 7,4 Gb/s (app mix)	Gb/s	7,4			spĺňa / 7,5 Gbps	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: Threat Prevention throughput (appmix)† 7.5 Gbps						
	Minimálny počet súbežných spojení musí dosahovať hodnotu min. 1 300 000	ks	1 300 000			spĺňa / 1 400 000 ks	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
Konkrétny text: Max concurrent sessions§ 1.4M							

	Minimálny počet nových spojení za sekundu musí dosahovať hodnotu min. 140 000	ks	140 000			spĺňa / 145 000 ks	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: New sessions per second 145,000						
Sieťová funkcionality:	NGFW musí plne podporovať IPv4 aj IPv6					spĺňa	https://docs.paloaltonetworks.com/compatibilitymatrix/reference/ipv6-support-by-feature
	NGFW musí podporovať zapojenie v režimoch L2 (s virtuálnym L3 rozhraním), L3, transparent a TAP					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať preklady adresy typu Static NAT, Dynamic NAT, PAT, NAT64 a perzistentné NAT pre DIPP (Dynamic IP and Port)					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať MSDP (Multicast Source Discovery Protocol) pre pokročilé smerovanie a BFD (Bidirectional Forwarding Detection) pre tradičné aj pokročilé smerovanie.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networkingadmin/advanced-routing/configure-msdp
	NGFW musí podporovať nástroj pre pokročilé smerovanie (Advanced Routing Engine)					spĺňa	https://docs.paloaltonetworks.com/ngfw/networking/advanced-routing
	PBR musí byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, užívateľ.					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/policy-basedforwarding
	NGFW musí umožniť nakonfigurovať expiračnú dobu cookies na 1 až 5 rokov					spĺňa	https://docs.paloaltonetworks.com/pan-os/10-1/panos-new-features/networking-features/lsvpn-cookieexpiry-extension
	NGFW musí podporovať web proxy funkcionality.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-3400-series
	NGFW musí podporovať stateful DHCPv6 klienta na získanie IPv6 adresy a iných parametrov					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-networking-admin/dhcp/firewall-as-a-dhcpv6-client
	NGFW musí umožniť nakonfigurovať IPSec tunel v transportnom móde na šifrovanie komunikácie medzi hosťami a IPSec tunnel s podporou post-quantum šifrovania priamo na NGFW bez nutnosti použitia tretích strán.					spĺňa	Na úvodnej strane dokument popisuje požadovanú vlastnosť: https://docs.paloaltonetworks.com/network-security/quantum-security/administration/configure-quantum-resistant-ikev2-vpns
	Konkrétny text: Quantum-resistant IKEv2 VPNs based on RFC 8784 or RFC 9242 and RFC 9370 prevent attackers who attempt to execute Harvest Now, Decrypt Later attacks from stealing the cryptographic key material used to encrypt data in the VPN.						

	NGFW musí podporovať výmenu hybridných post quantových kľúčov založených na RFC 9242 a RFC 9370 v rámci IKEv2 a IPsec rekey a vytváranie hybridných post quantových kľúčov použitím kryptografických sád NIST round 3 a round 4.					spĺňa	Na úvodnej strane dokument popisuje požadovanú vlastnosť: https://docs.paloaltonetworks.com/network-security/quantum-security/administration/configure-quantum-resistant-ikev2-vpns
	Konkrétny text: Quantum-resistant IKEv2 VPNs based on RFC 8784 or RFC 9242 and RFC 9370 prevent attackers who attempt to execute						
	NGFW musí podporovať súčasne na jednom zariadení na úrovni sieťového rozhrania konfigurácie Span, Transparent, Layer 3 a Layer 2.					spĺňa	Dokument popisuje vlastnosti v prvom odseku v druhej vete: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-interfaces/firewall-interfaces-overview
	Konkrétny text: you can configure the Ethernet interfaces on a firewall for virtual wire, Layer 2, Layer 3, and tap mode						
	NGFW musí umožniť segmentáciu a izoláciu sieťových zdrojov v rámci jedného fyzického zariadenia, čím sa zvyšuje bezpečnosť a efektivita správy prostredníctvom vytvárania viacerých virtuálnych firewallov.					spĺňa	Dokument detailne popisuje nasadenie a alokáciu zdrojov na virtuálne systémy https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/device/device-virtual-systems
	Konkrétny text: Virtual system (vsys) is an independent (virtual) firewall instance that you can separately manage within a physical firewall.						
VPN:	NGFW musí podporovať site-to-site VPN pomocou protokolu IPsec. Počet tunelov nesmie byť licenčne obmedzený					spĺňa	Dokument popisuje z high-level pohľadu nasadenie IPsec VPN tunelov. Licenčná politika Palo Alto Networks na NGFW neobsahuje možnosť rozšíriť počet tunelov, nakoľko nie sú limitované. https://docs.paloaltonetworks.com/network-
	Konkrétny text: A VPN connection that allows you to connect two local area networks (LANs) is called a site-to-site VPN						
	NGFW musí podporovať Remote Access VPN pomocou protokolov IPsec a SSL (min. TLS v1.2)					spĺňa	V prvom odstavci je uvedená podpora pre IPsec aj SSL: https://docs.paloaltonetworks.com/globalprotect/administration/globalprotect-cryptography Nasledne v tomto dokumente sú uvedené podporované TLS verzie: https://docs.paloaltonetworks.com/ngfw/administration/certificate-management/configure-ssl-tls-service-profile
	Konkrétny text: GlobalProtect supports both IPsec and SSL tunnel modes.						
	Konkrétny text: For the Max Version, select the latest allowed TLS version: TLSv1.0, TLSv1.1, TLSv1.2						
	Počet súčasne pripojených užívateľov nesmie byť licenčne obmedzený					spĺňa	Uvedené licencované vlastnosti Global Protect VPN klienta neuvádzajú obmedzenie na počet používateľov: https://docs.paloaltonetworks.com/globalprotect/activation-and-onboarding/your-globalprotect-license/your-globalprotect-license-ngfw
	Konkrétny text: If you want to use GlobalProtect to provide a secure remote access or VPN solution via single or multiple internal/external gateways, you don't need any GlobalProtect licenses.						
	NGFW musí pre Remote Access VPN poskytovať pripojenie z klientskych operačných systémov Windows a macOS					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?path=/content/pan/en_US/resources/datasheets/globalprotect-datasheet

	Priepustnosť IPSec musí byť min. 6,4 Gb/s	Gb/s	6,4			spĺňa / 6,6 Gbps	Datasheet na uvedenej stránke (Download) PA-3400 Series obsahuje detailne parametre navrhovaného zariadenia: https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series
	Konkrétny text: IPsec VPN throughput 6.6 Gbps						
Správa riešení:	Jednotlivé HW appliance musí obsahovať plnohodnotné grafické rozhranie (GUI) pre správu sieťových a bezpečnostných funkcií bez nutnosti používania centrálného manažment servera.					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-admin/firewall-administration/use-the-webinterface
	GUI musí podporovať čítanie logových záznamov bez nutnosti používania centrálného manažment servera.					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs
	Pripojenie ku GUI musí podporovať šifrovanie TLSv1.3					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-new-features/management-features/tls13-support-for-administrative-access
	NGFW musí byť spravovateľný pomocou GUI alebo CLI pričom GUI a CLI musí mať tzv. feature parity, poskytovať rovnaké možnosti konfigurácie.					spĺňa	Dokument popisuje možnosti konfigurácie PAN-OS Web-UI, CLI, API a Panoramu, každá oblasť odkazuje na samostatnú dokumentáciu: https://docs.paloaltonetworks.com/ngfw/administration/firewall-administration
	Konkrétny text: Administrators can configure, manage, and monitor Palo Alto Networks firewalls using the web interface, CLI, and API management interface.						
	Jednotlivé HW alebo SW zariadenia musia obsahovať plnohodnotné textové rozhranie (CLI) pre správu a čítanie logových záznamov bez nutnosti používania centrálného manažment servera. Vzdialené pripojenie k CLI musí podporovať šifrovanie (SSH)					spĺňa	https://docs.paloaltonetworks.com/ngfw/pan-os-cli-quick-start/get-started-with-the-cli
	Jednotlivé HW appliance musí obsahovať plnohodnotné API rozhranie na čítanie a konfiguráciu sieťových nastavení, bezpečnostných a ďalších pravidiel, nastavenia sieťových rozhraní a smerovania.					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-panorama-api/get-started-with-the-pan-os-xmlapi/explore-the-api
	Jednotlivé HW appliance musí umožňovať automatickú konfiguráciu nových NGFW použitím konfiguračných šablón na pripojenom USB flash disku.					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/firewalladministration/bootstrap-the-firewall/usb-flash-drivesupport
	NGFW musí pre autentizáciu a autorizáciu administrátorov podporovať protokoly LDAP, Radius, TACACS+, Kerberos a osobný certifikát					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/firewalladministration/manage-firewalladministrators/administrative-authentication
	NGFW musí obsahovať natívne nástroje pre debugging problémových situácií v úrovni L2 – L7 ISO/OSI modelu					spĺňa	Dokument presne popisuje ako vykonávať zachytávanie paketov a tým vykonávať debuging na celej úrovni OSI/ISO modelu: https://docs.paloaltonetworks.com/ngfw/administration/monitoring/take-packet-captures/take-a-custom-packet-capture
	Konkrétny text: Custom packet captures allow you to define the traffic that the Next-Generation Firewall will capture.						
	NGFW musí podporovať natívny nástroj na odchytenie prevádzky v GUI a CLI.					spĺňa	Dokument komplexne popisuje ako vykonať packet capture v GUI a CLI: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITJCA0
	Konkrétny text: advanced tools at the disposal of an admin is the ability to perform packet captures						

	NGFW musí byť možné spravovať z administrátorských staníc s OS Windows a macOS (vrátane HW s čipom Apple Silicon)					spĺňa	Dokument v uvode popisuje požiadavky na klientský SW na správu FW, čo sú bežne dostupné prehliadače dostupné na všetkých OS: https://docs.paloaltonetworks.com/ngfw/administration/firewall-administration/launch-the-web-interface
	Konkrétny text: The following web browsers are supported for access to the web interface						
	NGFW management musí podporovať prácu viacerých administrátorov v rovnakom čase, vrátane aplikácie politík a nastavení vytvorených iba konkrétnym administrátorom					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-web-interface-help/web-interface-basics/commitchanges
	NGFW musí obsahovať funkciu Policy Optimizer, ktorá dokáže automaticky optimalizovať a migrovať L4 bezpečnostnú politiku na L7 s identifikáciou aplikácií.					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-admin/app-id/security-policy-rule-optimization
	Natívne konfiguračné rozhraní (API) NGFW musí podporovať štandard OpenConfig bez nutnosti použitia treťostranného nástroja.					spĺňa	https://docs.paloaltonetworks.com/openconfig
Aplikačná kontrola:	NGFW musí podporovať aplikačnú detekciu a kontrolu ako svoju natívnu funkcionálnu					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/app-id/app-id-overview
	Priradenie povolenej či zakázanej aplikácie musí byť natívnou súčasťou vytvárania štandardného bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/security-rules
	NGFW musí podporovať identifikáciu aplikácií naprieč všetkými portami/protokolmi					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/app-id/applicationdefault#id86c929c8-01ad-49a0-9201-e56e7466a188
	NGFW musí podporovať identifikáciu aplikácií na neštandardných portoch					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/app-id/applicationdefault#id86c929c8-01ad-49a0-9201-e56e7466a188
	NGFW musí detekovať a zabrániť aplikácii meniť porty, tzv. port-hopping					spĺňa	Dokument komplexne popisuje správanie sa App-ID funkcionality, ktorá zabezpečuje identifikáciu konkrétnych aplikácií a zabráneniu rôznych útokov vrátane port-hoppingu: https://docs.paloaltonetworks.com/ngfw/administration/app-id/application-default
	Konkrétny text: Application-default is a feature of Palo Alto Networks firewalls that gives you an easy way to prevent this type of evasion and safely enable applications on their most commonly-used ports						
	NGFW musí umožňovať tvorbu plnohodnotných, užívateľsky definovaných signatúr aplikácií bez nutnosti využitia externého nástroja alebo zásahu výrobcu/dodávateľa					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/app-id/use-applicationobjects-in-policy/create-a-custom-application
	NGFW musí umožňovať zakázať inštaláciu nových signatúr aplikácií z aktualizácií poskytovaných vendorom					spĺňa	https://docs.paloaltonetworks.com/pan-os/10-1/panos-upgrade/software-and-content-updates/app-andthreat-content-updates
Kontrola na úrovni užívateľských identít:	NGFW musí podporovať vytváranie bezpečnostných pravidiel na základe užívateľských identít					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/security-rules com/ngfw/administration/app-id/app-id-overview
	NGFW musí umožniť blokovanie použitia korporátnej identity (kombinácia login a heslo) používateľa v externých službách a aplikáciách mimo organizáciu.					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/configuring-urlfiltering/configure-url-filtering
	Voľba užívateľskej identity musí byť natívnou súčasťou vytvárania štandardného bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/security-rules

NGFW musí umožňovať automaticky presun užívateľa do inej skupiny na základe bezpečnostného incidentu vzťahujúceho sa k danému užívateľovi, bez nutnosti manuálnej intervencie					spĺňa	https://docs.paloaltonetworks.com/networksecurity/securitypolicy/administration/objects/dynamic-user-groups
NGFW musí podporovať získavanie väzby IP adresa-užívateľské meno, bez nutnosti inštalácie klienta na koncové zariadenie, bez nutnosti inštalácie klienta na doménový kontrolér a bez nutnosti inštalácie ďalších komponentov mimo samotnej HW appliance					spĺňa	Dokument na úvodnej strane popisuje v odrážkach niekoľko alternatívnych spôsobov ako zabezpečiť požadovanú vlastnosť: https://docs.paloaltonetworks.com/ngfw/administration/user-id/map-ip-addresses-to-users
Konkrétny text: User-ID provides many different methods for mapping IP addresses to usernames.						
NGFW musí podporovať získavanie väzby IP adresa-užívateľské meno z Active Directory pomocou doménového účtu s čo najnižšími možnými právami na čítanie Security logů, bez nutnosti disponovať rizikovými úrovňami oprávnenia (napr. Domain Admins), zo systému Cisco ISE, prostredníctvom načítania informácie z logového záznamu, získaného pomocou zabezpečeného protokolu Syslog, z terminálových serverov MS (možné za pomoci nainštalovaného agenta), cez webový formulár - Captive Portal, VPN agenta, z NAC zariadenia (cez XML alebo API), z X-Forwarded-For (XFF) hlavičiek					spĺňa	Dokument na úvodnej strane popisuje v konkrétnych odrážkach všetky spôsoby ako zabezpečiť požadované funkcionality: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000scMcCAI https://docs.paloaltonetworks.com/ngfw/administration/user-id/map-ip-addresses-to-users
Konkrétny text: Use a dedicated service account for User-ID services with the minimal permissions necessary to connect the server monitoring. ...you can begin configuring user mapping using one or more of the following methods as needed to enable user-based access and visibility to applications and resources:						
ZTNA funkcionality musí byť realizovateľá priamo na NGFW bez nutnosti inštalácie ďalších komponentov, ktoré majú samostatný management.					spĺňa	Dokument popisuje a graficky znázorňuje ako zabezpečiť ZTNA funkcionality prostredníctvom HIP funkcionality v Global Protect agentovi priamo na NGFW: https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/globalprotect-for-internal-hip-checking-and-user-based-access
Konkrétny text: When used in conjunction with User-ID and/or HIP checks, an internal gateway provides a secure, accurate method of identifying and controlling traffic by user and/or device state, replacing other network access control (NAC) services. Palo Alto Networks ZTNA: https://www.paloaltonetworks.com/sase/ztna						
NGFW musí podporovať službu, ktorá dokáže konzistentne overovať a autorizovať všetkých používateľov bez ohľadu na umiestnenie a miesto uloženia identity používateľa (miestne, cloudové alebo hybridné). Podpora autentifikačných a autorizačných mechanizmov SAML a OpenID Connect.					spĺňa	Cloud Identity Engine je riešenie pre zabezpečenie požadovanej funkcionality, v ľavom menu s názvom Authenticate Users with the Cloud Identity Engine sa nachádzajú popisy ako zabezpečiť SAML a OpenID Connect autentifikáciu: https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/get-started-with-the-cloud-identity-engine
Konkrétny text: by continually syncing the information from your directories, whether they are on-premise, cloud-based, or hybrid, ensures that your user information is accurate and up to date and policy enforcement continues based on the mappings even if the cloud identity provider is temporarily unavailable. To authenticate users, configure a profile for a SAML 2.0-compliant identity provider (IdP) such as Google, Azure, Okta, PingOne, or PingFederate in the Cloud Identity Engine.						

	NGFW riešenie musí umožňovať redistribúciu identít používateľov z NGFW, kde je používateľ autentifikovaný na ostatné NGFW bez nutnosti inštalácie ďalších komponentov, ktoré majú samostatný management.					spĺňa	Dokument komplexne popisuje postup konfigurácie redistribúcie používateľských identít: https://docs.paloaltonetworks.com/ngfw/administration/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/configure-user-id-redistribution
	Konkrétny text: Data redistribution consists of: The redistribution agent that provides information The redistribution client that receives information						
	NGFW musí podporovať kontrolu klientskych staníc v pravidelných intervaloch cez Windows Management Instrumentation (WMI) alebo NetBIOS aby zistil, či je väzba IP adresa-užívateľské meno stále platná					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/user-id/user-idconcepts/user-mapping/client-probing
SSL/TLS Dešifrovanie :	NGFW musí podporovať dešifrovanie odchádzajúcej SSL/TLS prevádzky, za pomoci podvrhnutia serverového certifikátu klientom a naimportovaného privátneho kľúča interného servera					spĺňa	https://docs.paloaltonetworks.com/networksecurity/decryption/administration/decryptionoverview/ssl-forward-proxy
	NGFW musí podporovať dešifrovanie Secure Shell (SSH proxy) a kontrolovať tunelované aplikácie					spĺňa	https://docs.paloaltonetworks.com/networksecurity/decryption/administration/decryptionoverview/ssh-proxy
	Dešifrovanú prevádzku musí byť možné definovať na základe URL kategórií, aj všetkých ďalších typických parametrov, ako sú zdrojová a cieľová IP adresa, port, užívateľská identita					spĺňa	https://docs.paloaltonetworks.com/networksecurity/decryption/administration/decryptionoverview/decryption-policy-rules
	NGFW musí podporovať dešifrovanie za pomoci ECC (Elliptical Curve Cryptography), vrátane DHE a ECDHE pre prichádzajúcu i odchádzajúcu prevádzku					spĺňa	https://docs.paloaltonetworks.com/networksecurity/decryption/administration/decryptionoverview/decryption-profiles
	NGFW musí podporovať dešifrovanie protokolu TLS verzie 1.3					spĺňa	https://docs.paloaltonetworks.com/networksecurity/decryption/administration/decryptionoverview/tls-1-3-ssl-decryption
	NGFW musí podporovať preposielanie dešifrovanej prevádzky na iné skenovacie zariadenia tretích strán napr. DLP, analýza prevádzky a súborov a pod. Zariadenie 3 strany následne prepošle čisto prefiltrované dáta späť do NGFW. (tzv. decryption broker)					spĺňa	https://docs.paloaltonetworks.com/pan-os/10-1/panos-new-features/networking-features/networkpacket-broker
	NGFW musí podporovať preposielanie dešifrovanej prevádzky na špecifický port pre potreby archivácie prevádzky.					spĺňa	Dokument kompletne popisuje inštaláciu a použitie Network Packet Broker, funkcionality, ktorá spĺňa danú požiadavku: https://docs.paloaltonetworks.com/pan-os/10-1/panos-new-features/networking-features/network-packet-broker
	Konkrétny text: The new Network Packet Broker feature replaces Decryption Broker and expands its capabilities to filter and forward not only decrypted TLS traffic, but also non-decrypted TLS and non-TLS traffic, to one or more third-party appliances (a security chain).						
	NGFW musí podporovať OCSP (Online Certificate Status Protocol) na skontrolovanie platnosti SSL/TLS certifikátov v sieťovej architektúre obsahujúcej web proxy					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/certificatemanagement/certificate-revocation/online-certificatestatus-protocol-ocsp
Ochrana proti DoS:	NGFW musí obsahovať natívnu službu pre ochranu proti útoku typu DoS pomocou limitácie počtu spojení na úrovni zdrojová a cieľová IP adresa a užívateľská identita					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dosprotection
QoS:	NGFW musí poskytovať možnosť prioritizácie prevádzky a obmedzenia využívanej šírky pásma na základe zdrojovej a cieľovej IP adresy, portu, užívateľskej identity, aplikácie, času (od – do, deň v týždni + čas a pod.) a DSCP					spĺňa	https://docs.paloaltonetworks.com/networksecurity/quality-of-service/administration/configureqos

Logovanie a reportovanie :	NGFW musí obsahovať lokálne úložisko logov a nástroj pre analýzu logov bez nutnosti využitia ďalšieho systému mimo GUI					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs
	NGFW musí podporovať agregované zobrazenie logov na základe jedného filtrovacieho pravidla, naprieč jednotlivými typmi logov, ako sú prevádzkové logy, logy bezpečnostných incidentov a logy prístupov na URL					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs
	NGFW musí podporovať preposielanie logov na zariadenia tretích strán a umožňovať výber preposielaných logov na úrovni bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-admin/monitoring/configure-log-forwarding
	NGFW musí umožňovať vytváranie vlastných reportov priamo z grafického rozhrania NGFW					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-1/panos-admin/monitoring/view-and-manage-reports/generate-custom-reports
Servisná podpora a licenčný plán:	NGFW musí podporovať licenčný model nezávislý od počtu ochraňovaných koncových systémov					spĺňa	Dokument popisuje dostupné dodatočné licencie licencie, ktoré je možné aktivovať na NGFW, žiadne licencovanie neuvádza potrebu navýšenia počtu chránených koncových systémov: https://docs.paloaltonetworks.com/ngfw/getting-started/ngfw-compatible-subscriptions
	Konkrétny text: The following Palo Alto Networks subscriptions unlock certain NGFW features or enable the NGFW to leverage a Palo Alto Networks cloud-delivered service (or both). Here you can read more about each service or feature that requires a subscription to work with the NGFW. To enable a subscription, you must first activate subscription licenses; once active, most subscription services can use Dynamic Content Updates to provide new and updated functionality to the NGFW.						
	Požadovaná záručná doba NGFW je min. 60 mesiacov od nasadenia zariadenia do prostredia obstarávateľa. Obstarávané riešenie NGFW musí v rámci záručnej doby poskytovať plnú funkčnosť a prevádzkovú kontinuitu, a to bez dodatočných finančných nákladov na licencie, aktualizácie, technickú podporu alebo iné nevyhnutné súčasti zabezpečujúce jeho správnu a bezpečnú prevádzku.	mesiac	60			spĺňa / 60 mesiacov	Poskytujeme záruku a podporu na 60 mesiacov.
Sandboxing:	Firewall musí podporovať možnosť odoslať do sandboxu na inšpekciu neznámej vzorky prechádzajúcej protokolom HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.					spĺňa	https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/advanced-wildfire-signatures
	Sandbox systém musí byť od rovnakého výrobcu ako je NGFW, ale nemusí byť HW súčasťou NGFW.					spĺňa	https://docs.paloaltonetworks.com/advanced-wildfire/ngfw-compatible-subscriptions/activate-subscription
	Sandbox systém musí byť schopný okamžite automaticky vytvoriť IPS/AV signatúry pre NGFW, v prípade, keď je testovaná vzorka vyhodnotená ako škodlivá.					spĺňa	Dokument popisuje v druhom odstavci akým spôsobom riešenie vytvára signatúry: https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/advanced-wildfire-signatures
	Konkrétny text: Advanced WildFire can detect zero-day malware across multiple protocols including web (HTTP/HTTPS), email (SMTP, IMAP, POP), FTP, and SMB traffic. Upon detection, it rapidly generates unique signatures that protect against future infections from these newly discovered threats.						
	Sandbox musí byť schopný automaticky upraviť kategórie používané URL databázy ak zistí, že testovaná vzorka je škodlivá a komunikuje na konkrétne URL.					spĺňa	Dokument popisuje ako navrhované WildFire Sandbox riešenie pracuje s URL linkami a mení globálne PAN-DB: https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/url-analysis
	Konkrétny text: The Advanced WildFire global cloud (U.S.) and regional clouds can analyze URLs, and by extension, email links, to provide standardized verdicts and reports through						

Sandbox musí poskytovať aktualizácie signatúr pre AV, Webfiltering, DNS, C&C.					spĺňa	Dokument popisuje ako WildFire Sandbox poskytuje Signatúry pre ďalšie komponenty: https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/advanced-wildfire-signatures
Konkrétny text: Advanced WildFire can detect zero-day malware across multiple protocols including web (HTTP/HTTPS), email (SMTP, IMAP, POP), FTP, and SMB traffic. Upon detection, it rapidly generates unique signatures that protect against future infections from these newly discovered threats.						
Sandbox musí podporovať operačné systémy Windows, Linux, MacOS a Android					spĺňa	https://docs.paloaltonetworks.com/advancedwildfire/administration/advanced-wildfireoverview/advanced-wildfire-file-typesupport/advanced-wildfire-file-type-support-complete
Report z analýzy odoslanej vzorky do sandboxu musí byť prístupný priamo z rozhrania NGFW					spĺňa	https://docs.paloaltonetworks.com/advancedwildfire/administration/monitor-wildfire-activity/viewwildfire-logs-and-analysis-reports
Aktualizácia zero-day signatúr musí byť inštalovaná do NGFW v reálnom čase, čiže s nulovým oneskorením					spĺňa	https://docs.paloaltonetworks.com/wildfire/uv/wildfire-whats-new/wildfire-features-in-panos-100/wildfire-real-time-signature-updates
NGFW musí byť schopný detegovať a zablokovať stiahnutie neznámeho škodlivého súboru v reálnom čase, bez toho, aby bol doručený na koncový bod.					spĺňa	Dokument detailne popisuje best practices pre nasadenie WildFire Sandbox riešenia pre ochranu koncového bodu tak aby neznámy škodlivý dokument nebol doručený na koncový bod: https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/firewall-forwarding
Konkrétny text: The firewall forwards unknown samples, as well as blocked files that match antivirus signatures, for Advanced WildFire analysis based on the configured WildFire Analysis profile settings						
NGFW musí byť schopný detegovať neznáme vzorky priamo na firewallle bez nutnosti napojenia na externé zariadenie alebo službu.					spĺňa	https://docs.paloaltonetworks.com/whats-new/newfeatures/may-2024/local-deep-learning-foradvanced-threat-prevention
NGFW musí podporovať sandboxing v cloude, ktorý využíva umelú inteligenciu na ochranu pred sofistikovanými útokmi.					spĺňa	https://docs.paloaltonetworks.com/advancedwildfire/administration/configure-advanced-wildfireanalysis/enable-advanced-wildfire-inline-cloudanalysis
Sandbox musí vedieť používať introspekciu VM (Virtual Machine) a pamäťovú analýzu, aby odhalil vysoko sofistikovaný malware. Zároveň vie predchádzať tomu, aby malware rozpoznal, že sa nachádza vo virtuálnom prostredí.					spĺňa	Dokument kompletne popisuje technológiu Intelligent Run-time Memory Analysis, ktorá zabezpečuje požadovanú funkcionlitu: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/wildfire-features/intelligent-run-time-memory-analysis
Konkrétny text: Advanced WildFire is a new subscription offering available on NGFWs operating PAN-OS 10.0 and later that provides access to Intelligent Run-time Memory Analysis: a cloud-based advanced analysis engine that complements existing static, and dynamic analysis engines, to detect and prevent evasive malware threats. Advanced threats rely on techniques such as environmental checks and obfuscation to bypass detection; additionally, they often display signs of bespoke design with ephemeral behaviors that lead to fast-dissemination throughout the network, after an attack has been initiated. By leveraging a cloud-based detection infrastructure, Intelligent Run-time Memory Analysis detection engines operate a wide array of detection mechanisms to target these highly-evasive malware. To keep up with the latest threats, Advanced WildFire analysis engines are updated and deployed automatically, without requiring the user to download content update packages or run resource intensive, appliance-based analyzers.						

	Sandbox musí používať inteligentnú analýzu bežiackej pamäte a zachytáva snímky v čase, keď prebieha podozrivá aktivita.					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-new-features/wildfire-features/intelligent-run-timememory-analysis
	Sandbox musí rozpoznávať, ktoré závislosti malware potrebuje na to, aby sa spustil a vie ich nasimulovať.					spĺňa	Dokument popisuje na úvodnom obrázku Dependency emulation, čo je požadovaná funkcionality: https://docs.paloaltonetworks.com/pan-os/11-0/panos-new-features/wildfire-features/intelligent-run-timememory-analysisnew-features/wildfire-features/intelligent-run-timememory-analysis
	Konkrétny text: Dependency emulation (v obrázku)						
Bezpečnosť né funkcionality	NGFW musí podporovať zavedenie tzv. pozitívneho bezpečnostného modelu – povolenie iba vybraných aplikácií a zákaz všetkých ostatných aplikácií, vrátane neznámej prevádzky					spĺňa	https://www.paloaltonetworks.com/blog/2017/05/fourreasons-use-app-id-next-generation-firewall/
	NGFW musí obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (IPS). Databáza IPS signatúr musí byť uložená priamo vo NGFW. Aplikácia IPS profilu musí byť granulárna, na úrovni bezpečnostného pravidla					spĺňa	Dokument popisuje funkciu Advanced Threat Prevention, ktorá chráni proti známym aj neznámym zraniteľnostiam. V ľavom menu je možné nájsť odkaz Configure Threat Prevention, ktorý popisuje ako konfigurovať ochranu na úrovni pravidla. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/about-advanced-threat-prevention
	Konkrétny text: Advanced Threat Prevention is an intrusion prevention system (IPS) solution that can detect and block malware, vulnerability exploits, and command-and-control (C2) across all ports and protocols, using a multi-layered prevention system with components operating on the firewall and in the cloud. The Threat Prevention cloud operates a multitude of detection services using the combined threat data from Palo Alto Networks services to create signatures, each possessing specific identifiable patterns, and are used by the firewall to enforce security policies when matching threats and malicious behaviors are detected. These signatures are categorized based on the threat type and are assigned unique identifier numbers. To detect threats that correspond with these signatures, the firewall operates analysis engines that inspect and classify network traffic exhibiting anomalous traits.						
	NGFW musí umožňovať tvorbu užívateľsky definovaných IPS signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/dodávateľa					spĺňa	https://docs.paloaltonetworks.com/advanced-threatprevention/administration/configure-threatprevention/custom-signatures
	NGFW musí obsahovať integrovaný systém ochrany proti prítomnosti vírusov a škodlivého kódu. Databáza AV signatúr musí byť uložená priamo vo NGFW. Aplikácia AV profilu musí byť granulárna, na úrovni bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/securityprofiles/security-profile-antivirus
	Antivírus musí byť schopný kontrolovať prevádzku v minimálne týchto aplikáciách - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/securityprofiles/security-profile-antivirus
	NGFW musí umožňovať tvorbu užívateľsky definovaných spyware signatúr bez nutnosti využitia externého nástroja alebo zásahu výrobcu/dodávateľa					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-web-interface-help/objects/objects-customobjects-spywarevulnerability
	NGFW musí podporovať možnosť zablokovania útoku využívajúceho známe C&C centrá aj v prípade, že je prevádzka šifrovaná a nie je možné vykonávať SSL dekrypciu					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/securityprofiles/security-profile-anti-spyware
	NGFW musí v bezpečnostných pravidlách podporovať použitie externých dynamických zoznamov (napr. IP, URL, domény...); NGFW musí poskytovať možnosť overiť na základe certifikátov pravosť týchto dynamických zoznamov					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-admin/policy/use-an-external-dynamic-list-inpolicy/external-dynamic-list

NGFW musí podporovať import SNORT signatúr manuálne a cez API.					spĺňa	Dokument popisuje ako vytvoriť vlastnú signatúru a v odrážkach jednotlivé postupy pre import cez API: https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/ips-signature-converter-for-panorama
Konkrétny text: Snort and Suricata are open-source intrusion prevention system (IPS) tools that use uniquely formatted rules to detect threats. The IPS Signature Converter enables you to leverage these rules for immediate threat protection by translating the IPS signatures into custom Palo Alto Networks threat signatures. You can then register the signatures on Palo Alto Networks firewalls in specified device groups and enforce policy using Vulnerability Protection and Anti-Spyware Security Profiles. Additionally, you can export rules that list IP address indicators of compromise (IOC) and use the resultant text file as an external dynamic list to enforce policy on the entries contained in the list.						
NGFW musí pre prístup ku kritickým aplikáciám, poskytovať možnosť vynútiť viacfaktorové overenie prostredníctvom webového portálu, bez ohľadu na to, či cieľová aplikácia podporuje viacfaktorovú autentizáciu; táto vlastnosť musí byť konfigurovateľná na úrovni bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/ngfw/administration/authentication/configure-multi-factor-authentication
NGFW musí poskytovať možnosť zabrániť odoslaniu doménových užívateľských prihlasovacích údajov do iných, než povolených URL kategórií, pre zabránenie phishingu					spĺňa	https://docs.paloaltonetworks.com/ngfw/netpro-2/objects/objects-security-profiles-url-filtering/usercredential-detection
NGFW musí podporovať analýzu DNS dotazu tzv. sinkhole funkcií, ktorá pri DNS dotaze na škodlivú doménu vráti podvrhnutú IP adresu pre detailnejšiu analýzu a zároveň sa stanica na pôvodnú malware stránku nedostane.					spĺňa	https://docs.paloaltonetworks.com/advanced-threatprevention/administration/configure-threatprevention/use-dns-queries-to-identify-infectedhosts-on-the-network/how-dns-sinkholing-works
NGFW musí vedieť zabrániť neznámych injekčným útokom ako je SQLi a Command Injection útoky pomocou strojového učenia.					spĺňa	https://docs.paloaltonetworks.com/advanced-threatprevention/administration/threat-prevention/aboutadvanced-threat-prevention
NGFW musí podporovať Local Deep Learning, ktorý poskytuje mechanizmus na vykonávanie rýchlej, lokálnej analýzy zero-day a ďalších vyvíjajúcich hrozieb založených na hlbokom učení.					spĺňa	https://docs.paloaltonetworks.com/whats-new/newfeatures/may-2024/local-deep-learning-foradvanced-threat-prevention
NGFW musí byť schopný odhaliť a zablokovat' neznámu C2 (Command&Control) komunikáciu (napr. CobaltStrike, Empire), na ktorú neexistuje detekčná vzorka (signatúra).					spĺňa	Dokument popisuje konfiguráciu Anti-spyware profilu, ktorý blokuje C2 komunikáciu: https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware
Konkrétny text: Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. Podrobný popis Cobalt Strike: https://www.paloaltonetworks.com/blog/network-security/netsec-ngfw-cobalt-strike/						
Detekcia neznámej komunikácie musí byť realizovaná priamo na NGFW bez nutnosti použitia aktualizovaných IPS vzoriek.					spĺňa	https://docs.paloaltonetworks.com/ngfw
NGFW musí obsahovať lokálne ML modely, ktoré v prípade detekcie podozrivej komunikácie odklonia túto premávku do cloudovej služby pre pokročilú analýzu pomocou ML a Deep Learning.					spĺňa	https://www.paloaltonetworks.com/cyberpedia/whatis-an-ml-powered-ngfw
NGFW musí poskytovať funkcionality pokročilej analýzy DNS dotazov proti technikám používajúcim DGA (domain generation algorithm), Stockpiled,Squatting Domains, Subdomain Reputation, Predictive Detection, Strategically Aged Domains, Wildcard DNS, Compromised DNS Zones, Dangling DNS, NXNSAttack, Ultra-slow DNS Tunneling, Domain Masquerading a Traffic Distribution System v reálnom čase.					spĺňa	https://docs.paloaltonetworks.com/dnssecurity/administration/about-dns-security/cloud-delivered-dns-signatures

	NGFW musí vedieť rozpoznať komunikáciu ukrytú v DoH (DNS-over-HTTPS) požiadavkách a aplikovať potrebné DNS bezpečnostné pravidlá v reálnom čase.					spĺňa	https://docs.paloaltonetworks.com/dnssecurity/administration/configure-dnssecurity/configure-dns-over-doh
	NGFW musí umožniť tvorbu užívateľsky definovaných signatúr pre hrozby založené na L3 a L4 hlavičkách.					spĺňa	https://docs.paloaltonetworks.com/pan-os/11-0/panos-web-interface-help/network/network-networkprofiles/network-network-profiles-zone-protection/l3-l4-header-inspection
	NGFW musí vykonávať inšpekciu nie len DNS dotazov ale aj DNS odpovedí a to v reálnom čase, na NGFW alebo pomocou cloudových detekčných mechanizmov.					spĺňa	https://docs.paloaltonetworks.com/dnssecurity/administration/about-dns-security
	NGFW musí proaktívne blokovat prístup k nesprávne nakonfigurovaným doménam pomocou automatického zisťovania a monitorovania verejných domén					spĺňa	https://docs.paloaltonetworks.com/dnssecurity/administration/configure-dnssecurity/enable-advanced-dns-security
	NGFW musí vedieť detekovať a kategorizovať unesené (hijacked) domény a nesprávne nakonfigurované domény cez metódy strojového učenia, a to v reálnom čase lokálne na NGFW, alebo pomocou cloudových detekčných enginov.					spĺňa	https://docs.paloaltonetworks.com/dnssecurity/administration/configure-dnssecurity/enable-advanced-dns-security
URL filtering:	NGFW musí obsahovať natívnu podporu pre využívanie databázy URL					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/url-filtering-basics
	URL databázy musí byť od rovnakého výrobcu ako je NGFW					spĺňa	https://docs.paloaltonetworks.com/ngfw/gettingstarted/ngfw-compatible-subscriptions
	NGFW musí byť schopný použiť URL kategóriu v definícii bezpečnostného pravidla					spĺňa	https://docs.paloaltonetworks.com/networksecurity/security-policy/administration/security-rules
	NGFW musí podporovať vytváranie užívateľsky definovaných kategórií, bez nutnosti využiť externý nástroj a bez nutnosti zásahu výrobcu/dodávateľa					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/configuring-url-filtering/urlcategory-exceptions/create-a-custom-url-category
	URL databázy musí byť dynamicky aktualizovaná na základe novo zistených URL, vedúcich na škodlivý obsah alebo C&C centra					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/url-filtering-basics/how-urlfiltering-
	URL databázy musí podporovať možnosť zaradenia do aspoň dvoch kategórií naraz pre jediné URL					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/url-filtering-basics/urlcategories
	NGFW musí umožňovať požiadať o rekategorizáciu nevhodne zaradených URL priamo v grafickom rozhraní NGFW bez nutnosti kontaktovania technickej podpory					spĺňa	https://docs.paloaltonetworks.com/advanced-urlfiltering/administration/monitoring/request-to-changethe-category-for-a-url
	NGFW musí obsahovať URL kategórie špecifické pre GenAI/LLM aplikácie a služby minimálne v rozsahu (Conversational Assistant, Writing Assistant, Media Service, Data And Workflow Optimizer, Meeting Assistant)					spĺňa	https://live.paloaltonetworks.com/t5/communityblogs/new-advanced-url-filtering-granular-artificialintelligence/ba-p/997295
	NGFW musí byť rozšíriteľný o ochranu prístupu ku GenAI/LLM službám a aplikáciám, ochrana musí byť priamo dostupná na NGFW a nesmie byť dodaná ako samostatné riešenie.					spĺňa	https://docs.paloaltonetworks.com/ai-access-security
IoT Security:	NGFW riešenie musí obsahovať natívnu (bez nutnosti inštalácie agentov alebo sieťových sond) funkcionality bezpečnosť IoT (automatizovaná identifikácia zariadení a ich zraniteľností, automatizované bezpečnostné pravidlá pre IoT) bez nutnosti integrácie s tretími stranami a nie je licenčne obmedzený počet chránených zariadení.					spĺňa	https://docs.paloaltonetworks.com/iot/gettingstarted/iot-security-solution
	Riešenie IoT bezpečnosti vyžaduje lokálne senzory v podobe obstarávaných NGFW.					spĺňa	https://docs.paloaltonetworks.com/iot/gettingstarted/iot-security-solution

Riešenie IoT bezpečnosti objavuje a identifikuje zariadenia v reálnom čase a zároveň je možné objavovanie naplánovať, pričom objavovanie sa vykonáva pasívne bez akéhokoľvek dopadu na cieľové zariadenia					spĺňa	https://docs.paloaltonetworks.com/iot/administration/disc-over-iot-devices-and-takeinventory
Riešenie IoT bezpečnosti cez NGFW senzor IoT získava sieťovú prevádzku z nasledujúcich zdrojov, aby objavil zariadenie IoT: DHCP traffic, NetFlow, SNMP, TAP, ERSPAN					spĺňa	Dokument detailne popisuje vlastnosti funkcionality Device-ID, rovnako ako požadované zdroje pre detekciu zariadení: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-id/device-id-overview
Konkrétny text: To identify devices with dynamically assigned network settings, the firewall must be able to observe DHCP broadcast and unicast traffic on your network. IoT Security also supports static IP devices. The more traffic the firewall can observe, the more accurate the policy rule recommendations are for the device and the more rapid and accurate the IP address-to-device mappings are for the device. When a device sends DHCP traffic to obtain its network settings, the firewall observes this type of request and generates EALs to send to the logging service, where IoT Security accesses them for analysis. Neflow: https://docs.paloaltonetworks.com/ngfw/administration/monitoring/netflow-monitoring SNMP: https://docs.paloaltonetworks.com/iot/getting-started/firewall-deployment-for-device-visibility/use-snm-network-discovery-to-learn-about-devices-from-switches TAP: https://docs.paloaltonetworks.com/network-security/device-id/administration/prepare-to-deploy-device-id ERSPAN: https://docs.paloaltonetworks.com/network-security/device-id/administration/prepare-to-deploy-device-id						
Riešenie využíva na identifikáciu a klasifikáciu zariadenia signatúry alebo tzv. "fingerprints" zariadenia.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/iot-security
Riešenie IoT bezpečnosti zisťuje a stanovuje základné správanie IoT zariadenia ako: úrovne patchovania zariadenia, detekuje a hlási aplikácie vrátane názvu a verzie, zisťuje a hlási verziu aplikačného softvéru, detekuje a hlási typy pripojenia, interné aj externé.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/iot-security
Riešenie IoT bezpečnosti porovná konfiguráciu s ostatnými zariadeniami v sieti a s ostatnými zariadeniami v databáze zariadení crowdsourced					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/iot-security
Riešenie IoT bezpečnosti deteguje zariadenia pre vzdialené monitorovanie pacienta (RPM) vysielajúce do zdravotníckych systémov EHR, zariadenia s odvolaním FDA, zariadenia s dátami chránených zdravotných informácií (PHI) a protokoly aplikácií telehealth, pričom zisťuje a hlási autentizáciu užívateľa, teda identifikuje, kto sa prihlasuje do zariadenia IoT.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/healthcare-iot-solution-brief
Riešenie IoT bezpečnosti automaticky udržiava knižnicu dokumentov a máp MDS2, prijíma dokumenty MDS2 pre zariadenia IoT a extrahuje kontext zariadení a rizík, a zároveň automaticky identifikuje rizikovú pozíciu na základe správania špecifikovaného výrobcom, napríklad chýbajúceho antivírusu alebo aktualizácie signatúr.					spĺňa	https://docs.paloaltonetworks.com/iot/administration/medical-iot-utilization
Riešenie IoT bezpečnosti sleduje nesprávnu konfiguráciu zariadenia, beh neobvyklého softvéru na IoT zariadeniach, pripájanie zariadení ku cloudu alebo sieti, použitie predvolených hesiel, prihlásenie tretej strany alebo výrobcu k zariadeniu, zariadenia, operačné systémy a aplikácie na konci životnosti (EOL), ako aj pripojenie zariadenia k menej zabezpečenému zariadeniu.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/iot-security
Riešenie IoT bezpečnosti sleduje históriu zraniteľnosti IoT zariadení, CVE, bezpečnosť „data-at-rest“ a zisťuje, či sú zariadenia IoT evidované v ICS-CERT. Porovnáva správanie zariadenia s inými crowdsourcingovými zariadeniami, sleduje aplikácie spôsobujúce znížený výkon siete, základné línie správania a zisťuje nepretržité chyby DHCP.					spĺňa	Dokument obsahuje v ľavej strane odkazy na detailný popis požadovaných funkcionalít ako Vulnerability Overview Dashboard, Risk Assessment, Virtual Patching atd. Tieto zabezpečujú požadované vlastnosti: https://docs.paloaltonetworks.com/iot/administration/detect-iot-device-vulnerabilities

Konkrétny text: A vulnerability refers to an intrinsic flaw built into the software or hardware of a device that is often well-known and can be exploited in some way. A risk, on the other hand, considers environmental, configuration, behavioral, and security policy-related factors in addition to one or more underlying vulnerabilities. This distinction is important because some risks appear in the device details page but not on the Vulnerabilities page, and yet they can influence the severity level that Device Security assigns to a vulnerability. Device Security considers a vulnerability to be potential when it applies to a specific device type, model, and version number and one or more devices match the specified device type but their model and/or version number are unknown. Similarly, a device is considered to be potentially vulnerable for the same reason. Dokument ICS/SCADA INDUSTRY Solutions Brief (Download) popisuje Threat Signatures for ICS/SCADA-Specific Vulnerabilities, ktoré su naviazane na ICS-CERT. https://www.paloaltonetworks.com/resources/techbriefs/scada-ics-solution-brief						
Riešenie IoT bezpečnosti deteguje podozrivé veľké množstvo nešifrovaných dátových prenosov, prenos veľkého množstva dát, porušenie zásad, abnormálnu prevádzku medzi zariadeniami a roaming stacionárnych zariadení. Automaticky identifikuje anomálie, ktoré nespádajú do správania stanoveného výrobcom, napríklad vzdialené aktualizácie softvéru.					spĺňa	https://docs.paloaltonetworks.com/iot/gettingstarted/iot-security-solution/iot-security-solutionstructure
Riešenie IoT bezpečnosti deteguje anomálie označujúce hrozby, pripojenie zariadenia ku škodlivým doménam, hrozby na BYOD (Bring Your Own Devices) IoT, známe IoT a IT hrozby na zariadeniach, neznáme hrozby, hrozby na základe rozsiahleho prieskumu priemyselných hrozieb, neúspešné pokusy o "brute-force" zadávania PIN, pripojenie osobného zariadenia k veľkému počtu zariadení indikujúcich zneužitie, výstrahy založené na signatúrach od NGFW, EPP a podobne, neobvyklé sieťové spojenia a nevhodné požiadavky na pripojenie.					spĺňa	Dokument v celom rozsahu detailne popisuje vlastnosti funkcionality Device-ID, ktorá spĺňa požiadavky: https://docs.paloaltonetworks.com/iot/getting-started/iot-security-solution/iot-security-solution-structure
Konkrétny text: Using AI and machine learning, Device Security automatically discovers and identifies all network-connected devices and constructs a data-rich, dynamically updating inventory. In addition to identifying IoT devices and IT devices (laptops and servers for example), Device Security provides deep visibility into network behaviors, establishing what's normal and discerning what's suspicious. When it detects a device vulnerability or anomalous behavior posing a threat, Device Security notifies administrators, who can then take action to investigate and remediate the issue.						
Riešenie IoT bezpečnosti poskytuje automatické odporúčania politik znižovania rizík na základe hodnotenia rizík a umožňuje priebežné sledovanie účinnosti týchto politik. Upozorňuje na zraniteľnosti, nesúlad zariadenia, hrozby, exploity a škodlivý obsah v komunikácii zariadenia, pričom upozornenia obsahujú dôležité informácie, ako je dátum, čas, typ a aktivity, ktoré ich vyvolali.					spĺňa	Uvedený odkaz referuje na PDF dokument (Download) What is vulnerability management for medical devices, ktorý popisuje požadované vlastnosti: https://www.paloaltonetworks.com/resources/datasheets/cdss-vulnerability-management-healthcare
Konkrétny text: CVEs Weak or default passwords Unsecure protocol usage Incorrect device usage End-of-life OS/Apps/Devices/Obsolete protocols Misconfiguration of IoT devices FDA recalls Third-party/Manufacturers logins attempts Decommissioned medical devices connected to the network Deviance from manufacturer specifications Risk indicators captured in MDS2 documents Devices storing or transmitting ePHI data Access to malicious domains Unusual software running Security policy violations Virtual Patching: https://docs.paloaltonetworks.com/iot/administration/detect-iot-device-vulnerabilities/virtual-patching-overview Konkrétny text: Virtual patching provides the capability to mitigate risks in OT and IoT environments						

Riešenie IoT bezpečnosti ponúka prispôsobiteľné úrovne rizika pre výstrahy a možnosť vyvážená skóre s existujúcim rámcom rizík zákazníka, umožňuje potlačenie výstrah pre určitý typ a podporuje generovanie vlastných upozornení.					spĺňa	https://docs.paloaltonetworks.com/iot/administration/respond-to-iot-security-alerts
Riešenie umožňuje automatické vytváranie výstražných tiketov v ticketingových systémoch (CMMS, ITSM) a automatické výstražné akcie v systéme NAC, ako je karanténa zariadenia. Umožňuje preskúmať výstrahy z riadiaceho panela pre proces s uzavretou slučkou, pričom schopnosť prevencie hrozieb je zabudovaná do senzora IoT alebo je možné ju dosiahnuť integráciou s riešením tretej strany.					spĺňa	https://docs.paloaltonetworks.com/iot/gettingstarted/iot-security-solution/iot-security-integrationswith-third-party-products
Riešenie IoT bezpečnosti poskytuje virtuálne zaplätanie rizikových zariadení, hlási profily zariadení, novo objavené zariadenia a informuje o zraniteľnostiach aktív, zásadách a overovaní aplikovaných bezpečnostných kontrol, ako aj poskytuje súhrnné správy o prevádzkových lekárskych prehľadoch a správy na základe priority rizík.					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/healthcare-iot-solution-brief
Riešenie IoT bezpečnosti poskytuje detekciu a prevenciu pred známymi a neznámymi (Zero Day) hrozbami					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/healthcare-iot-solution-brief
Riešenie IoT bezpečnosti poskytuje otvorenú API pre integráciu s riešeniami tretích strán, dodržiava regulačné normy a predpisy (napr. FDA, ECRI, ISO, NIST, ICS-CERT), zisťuje zhodu s bezpečnostnou smernicou SP 800-121 (Bluetooth) a sleduje zhodu s PHI na zariadeniach.					spĺňa	Uvedený odkaz referuje na dokumentáciu, ktorá popisuje Biomed Dashboard, ktorá spĺňa dané požiadavky: https://docs.paloaltonetworks.com/iot/administration/medical-iot-utilization/biomed-dashboard
Konkrétny text: Devices with outdated endpoint protection: These are devices that have endpoint protection, such as anti-virus protection, but they haven't communicated with their vendor and haven't been updated in over a month. This makes them vulnerable to new types of attacks released since their last update. Devices without endpoint protection: These are devices that do not have any endpoint protection installed on them. Devices with PHI: These devices contain personal health information (PHI). FDA Recall Instances: This shows the total number of devices that have been issued a recall order by the Food and Drug Administration (FDA) because of a product flaw that affects safety and requires it to be fixed or replaced. https://docs.paloaltonetworks.com/iot/administration/discover-iot-devices-and-take-inventory/discover-mobile-device-attributes Konkrétny text: Radio Access Technology – The underlying connection method mobile devices use for wireless radio communications; for example, Bluetooth, Wi-Fi, UMTS, LTE, or 5G NR						
Riešenie má vstavanú integráciu s IPAM (správa IP adries), ITSM (správa IT služieb), LDAP/AD (Active Directory), RTLS (real-time locating system), SIEM, SOAR, CMMS (počítačový systém riadenia údržby) a podporuje správu zraniteľností prostredníctvom integrácie s nástrojmi ako Qualys, Rapid7, Tenable, ako aj so zdrojmi zraniteľností (H-ISAC, ICS-CERT, MDISS a pod.).					spĺňa	https://docs.paloaltonetworks.com/iot/gettingstarted/iot-security-solution/iot-security-integrationswith-third-party-products
Riešenie IoT bezpečnosti má vstavanú integráciu s firewallom a NAC pre nasadenie bezpečnostných pravidiel a segmentácie, integráciu so segmentačnými prepínačmi, integráciu CMDB (databáza správy konfigurácie) pre udržiavanie aktuálneho inventára majetku, integráciu so systémami ERP (plánovanie podnikových zdrojov),					spĺňa	Externé integrácie sú natívnou súčasťou Device Security: https://docs.paloaltonetworks.com/iot/integration/get-started-with-iot-security-integrations
Konkrétny text: In addition to coordinating with Palo Alto Networks next-generation firewalls, Device Security integrates with third-party systems, augmenting their inventory, network management, network security, and vulnerability detection by making them IoT aware and by gathering device and network data from other sources to enrich its own inventory and capabilities. Device Security can integrate with the following third-party applications:						
Riešenie IoT bezpečnosti musí zobrazit využitie prístroja - CT skener, infúzný systém, MRI, zobrazovač nukleárnej medicíny, PET skener, ultrazvukový prístroj, RTG prístroj. Riešenie poskytuje informáciu o využití zariadenia v hodinách.					spĺňa	https://docs.paloaltonetworks.com/iot/administration/medical-iotutilization/utilization-dashboard

	Riešenie IoT bezpečnosti musí pre zariadenia umožniť generovať trendový graf snímkov urobených v daných intervaloch, trendový graf prípadových štúdií, analýzu skenovania obrazu a skenovanie dát podľa miesta.					spĺňa	Uvedený odkaz referuje na PDF dokument (Download) Medical IoT Security Solution Brief, ktorý popisuje požadované vlastnosti: https://www.paloaltonetworks.com/resources/techbriefs/healthcare-iot-solution-brief
	Konkrétny text: Improve patient experience and operations with business and clinical intelligence, helping you organize and optimize expensive resources. Biomedical and clinical teams often find themselves over budget while medical devices remain underutilized and maintenance costs soar. Medical IoT Security alleviates the pain of device purchase and preventive maintenance while saving costs on patient care by automatically tracking and reporting on connected medical device usage and resource allocation.						
	Riešenie IoT bezpečnosti poskytuje prehľad o celkovom počte zariadení v sieti za posledný rok, vrátane počtu zariadení, ktoré boli pripojené a použité, pripojené, ale nepoužívané (len online), alebo odpojené (offline).					spĺňa	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/healthcare-iot-solution-brief
Položka č. 2 Služby spojené s dodávkou Firewall		parametre					
		MJ	min.	max.	presne		
2.1	Analýza a dizajn (analýza súčasného stavu, návrh riešenia). Počet mesiacov od dodania všetkých HW a SW komponentov (Položky č. 1 a č. 2)	mes.		2		spĺňa / 2 mesiace	
2.2	Implementácia a testovanie (inštalácia zariadení, FAT a SAT testy, konfigurácia zariadení, zapojenie do režimu vysokej dostupnosti, integrácia do nadradených nástrojov SIEM). Počet mesiacov od ukončenia míľníka Analýza a dizajn (Položka 2.1).	mes.		6		spĺňa / 6 mesiace	
2.3	Nasadenie a PIP (Optimalizácia konfigurácie v prevádzke, postimplementačná podpora - dohľad) Počet mesiacov od ukončenia míľníka Implementácia a testovanie (Položka 2.2)	mes.		4		spĺňa / 4 mesiace	
2.4	Dodanie dokumentácie					spĺňa	
2.5	Zaškolenie obsluhy (2 zamestnanci obstarávateľa)	hod.	8			spĺňa / 8 hod.	

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby Jozef Dobiš
 podpis a
 pečiatka

Príloha č. 6 súťažných podkladov

Názov predmetu zákazky: **Technológie sieťovej a komunikačnej bezpečnosti**

NÁVRH NA PLNENIE KRITÉRIA - KALKULÁCIA CENY

Por. č.	Predmet zákazky	Merná jednotka (MJ)	Množstvo	Obchodný názov ponúkaného produktu	Názov výrobcu ponúkaného produktu	ŠUKL kód	Jednotková cena v EUR				Celková cena za požadovaný počet MJ v EUR			
							bez DPH	sadzba DPH v %	suma DPH v EUR	s DPH	bez DPH	sadzba DPH v %	suma DPH v EUR	s DPH
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
1.	Firewall	ks	2	Palo Alto FW PA-3410	Palo Alto Networks		103 000,00 €	23%	23 690,00 €	126 690,00 €	206 000,00 €	23%	47 380,00 €	253 380,00 €
2.	Služby spojené s dodávkou firewall	ks	1		implementácia		30 000,00 €	23%	6 900,00 €	36 900,00 €	30 000,00 €	23%	6 900,00 €	36 900,00 €

Obchodný názov uchádzača:	SmartSec Technologies s.r.o.
Sídlo uchádzača:	Jégeho 6, Bratislava 821 08
IČO:	50448676
DIČ:	2120361452
IČ DPH:	SK2120361452

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby Jozef Dobiš, konateľ
podpis a pečiatka uchádzača

Príloha č. 7 súťažných podkladov

Názov predmetu zákazky: **Technológie sieťovej a komunikačnej bezpečnosti**

Zoznam dodaných tovarov

Uchádzač: SmartSec Technologies s.r.o., Jégeho, Bratislava 821 08

(uviest' obchodné meno a sídlo uchádzača alebo miesto podnikania)

Zoznam dodaných tovarov za predchádzajúce 3 roky od vyhlásenia verejného obstarávania

Obchodné meno/názov zmluvného partnera, adresa jeho sídla alebo miesta podnikania, IČO	Názov/stručný opis predmetu zákazky	Cena za dodaný tovar v EUR bez DPH resp. v EUR s DPH	Lehota dodania tovaru (mesiac a rok)	Odberateľ - kontaktná osoba, meno, priezvisko, telefónne číslo, e-mail
Štátny veterinárny a potravinový ústav Jánoškova 58, 026 01 Dolný Kubín IČO: 42 355 613	Dodávka firewallov, centrálneho manažmentu a implementácia riešenia	58 323,00 €	07/2023	https://www.uvo.gov.sk/udaje-o-hospodarskych-subjektoch-vedene-uradom/evidencia-referencii/detail-referencia/dokument/1333040?
Slovenská pošta, a.s. Partizánska cesta 9, 975 99 Banská Bystrica IČO: 36 631 124	Podľa Rámcovej dohody 77/2023 o dodaní hardvéru Aplikačný Firewall F5 - dodávka a implementácia	294 400,00 €	08/2023	Pavel Považanec povazanec.pavel@slposta.sk

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby Jozef Dobiš
podpis a pečiatka

KÚPNA ZMLUVA

uzatvorená podľa § 409 a nasl. zák. č. 513/1991 Zb. Obchodný zákonník, v znení neskorších predpisov (ďalej len „Zmluva“)

čl. I. Zmluvné strany

1. Kupujúci : **Univerzitná nemocnica L. Pasteura Košice**
v zastúpení: MUDr. Ľuboslav Beňa, PhD., MPH - riaditeľ
sídlo: Rastislavova 43, 041 90 Košice, SR
IČO: 00 606 707
DIČ: 2021141969
IČ DPH: SK2021141969
Bankové spojenie: Štátna pokladnica, Radlinského 32, 810 05 Bratislava
IBAN: SK 06 8180 0000 0070 0028 0550
SWIFT: SPSRSKBA
Štátna príspevková organizácia zriadená Zriaďovacou listinou Ministerstva
zdravotníctva SR č. 1842/1990-A/I-2 zo dňa 18. 12. 1990

(ďalej len „kupujúci“)

2. Predávajúci : **SmartSec Technologies s.r.o.**
v zastúpení: Ing. Jozef Dobiš, konateľ
sídlo: Jégeho 6, Bratislava 821 08
IČO : 50448676
DIČ: 2120361452
IČ DPH: SK2120361452
Bankové spojenie: Tatra banka a.s.
IBAN : SK76 1100 0000 0029 4702 8013
SWIFT : TATRSKBX
Zapísaný v Obchodnom registri Mestského súdu BA III., odd. : Sro,
Vložka č. : 114228/B

(ďalej len „predávajúci“)

Čl. II. Úvodné ustanovenia

1. Kupujúci v rámci plnenia svojich úloh obstaráva tovar postupom stanoveným zákonom č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov (ďalej len „zák. č. 343/2015 Z. z.“).
2. Túto zmluvu uzatvára kupujúci, ktorý je verejným obstarávateľom s predávajúcim, ktorý je úspešným uchádzačom ako výsledok verejného obstarávania postupom zadávania nadlimitnej zákazky podľa § 66 ods. 7 zák. č. 343/2015 Z. z. realizovanej prostredníctvom systému elektronického verejného obstarávania JOSEPHINE zverejnenej vo Vestníku verejného obstarávania č. 174/2025 zo dňa 28.08.2025 pod. zn. 14025 – MST na predmet zákazky s názvom „Technológie sieťovej a komunikačnej bezpečnosti,“ (ďalej len „verejné obstarávanie“) v súlade s ponukou predávajúceho zo dňa 26.09.2025.
Evidenčné číslo verejného obstarávania kupujúceho : UNLP-2025-83-NZ-VS
3. Kupujúci je poskytovateľom zdravotnej starostlivosti podľa zák. č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov.
4. Predávajúci prehlasuje, že je oprávnený disponovať s tovarom v zmysle tejto zmluvy.
5. Tovar, ktorý je predmetom plnenia tejto zmluvy bude hradený z finančných prostriedkov, ktoré kupujúci ako verejný obstarávateľ dostal na základe **Zmluvy o poskytnutí nenávratného finančného príspevku, číslo zmluvy: 33/2025 zo dňa: 27.1.2025**, ktorá bola uzatvorená medzi kupujúcim ako prijímateľom a Ministerstvom investícií, regionálneho rozvoja a informatizácie

Slovenskej republiky ako Poskytovateľom (ďalej len „Zmluva o poskytnutí prostriedkov“), (Zmluva o poskytnutí nenávratného finančného príspevku bola dňa 28.1.2025 zverejnená v CRZ: <https://www.crz.gov.sk/zmluva/10349356/?csrt=11539501529182901473&undefined=undefined>) a čiastočnej aj z vlastných finančných prostriedkov kupujúceho, ak táto povinnosť, vzhľadom na maximálnu výšku poskytnutých finančných prostriedkov na základe Zmluvy o poskytnutí prostriedkov vznikne kupujúcemu po uzatvorení tejto zmluvy.

Názov projektu: Realizácia opatrení kybernetickej a informačnej bezpečnosti UNLP Košice

Kód výzvy: PSK-MIRRI-615-2024-DV-EFRR

Kód projektu: 401101A575

Program: 401000 - Program Slovensko - SK - EFRR/KF/FST/ESF+

Priorita: 401101 - 1P1 Veda, výskum a inovácie

Špecifický cieľ: 401101R102 - RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy

Celková suma oprávnených výdavkov: 292 737,80 EUR s DPH

Čl. III. Predmet zmluvy

1. Predávajúci sa touto zmluvou zaväzuje dodať kupujúcemu tovar podľa bodu 2. tohto článku a previesť na neho vlastnícke právo k tomuto tovaru a kupujúci sa zaväzuje zaplatiť za tovar kúpnu cenu podľa tejto zmluvy.
2. Tovarom pre účely tejto zmluvy je dodanie Firewallu (ďalej len „tovar“) a služieb spojených s dodávkou Firewallu (ďalej len „služby“) podľa špecifikácie uvedenej **v prílohe č. 1** tejto zmluvy.
3. Dodanie tovaru zahŕňa aj licencie, ich aktualizácie, technickú podporu a iné nevyhnutné súčasti zabezpečujúce správnu a bezpečnú prevádzku predmetu plnenia.
4. Tovar sa dodáva za účelom zabezpečenia bezpečnosti prevádzky IS a sietí, vrátane sieťovej a komunikačnej bezpečnosti v kritickej infraštruktúre.

Čl. IV. Dodacie podmienky

1. Predávajúci sa zaväzuje dodať tovar vrátane služieb podľa článku III. bod 2. a 3. tejto zmluvy kupujúcemu do 14 mesiacov odo dňa účinnosti tejto zmluvy. Konkrétny termín dodania tovaru oznámi predávajúci kupujúcemu najmenej dva pracovné dni vopred, a to písomne na e-mailovú adresu: vagas@unlp.sk, tomas.kaszoniy@unlp.sk a telefonicky na tel. č.: +421 , +421 !
2. Miesto dodania tovaru je pracovisko kupujúceho: Odbor informačných a komunikačných technológií, Rastislavova 43, Košice.
3. Predávajúci je povinný dodať tovar podľa špecifikácie uvedenej v prílohe č. 1 tejto zmluvy nový, nepoužívaný, v originálnom balení, kompletný (nie po častiach) a v minulosti neregistrovaný u iného užívateľa.
4. Dodanie tovaru do miesta dodania potvrdzuje kupujúci písomne, a to podpísaním preberacieho protokolu/dodacieho listu. V **Preberacom protokole/dodacom liste** sa potvrdzuje druh, množstvo, vyhotovenie a kompletnosť dodaného tovaru podľa špecifikácie uvedenej **v prílohe č. 1 tejto zmluvy**. V prípade zistenia väd tovaru pri jeho prevzatí je kupujúci oprávnený tovar neprevziať.
5. Osobou oprávnenou na prevzatie tovaru za kupujúceho (oprávnený na podpísanie Preberacieho protokolu/dodacieho listu) je : Ing. Pavel Vagaš, MPH, e-mail adresa: vagas@unlp.sk, tel. č. +421
6. Predávajúci je povinný dodať a nainštalovať tovar na miesto dodania tovaru na vlastné náklady. Kupujúci je povinný poskytnúť predávajúcemu potrebnú súčinnosť a umožniť uvedenie tovaru do prevádzky.
7. Kupujúci je povinný podať správu predávajúcemu o vadách tovaru bez zbytočného odkladu po tom, čo sa vady mohli zistiť.
8. Kupujúci je oprávnený odmietnuť prevzatie tovaru, ak technické a funkčné parametre dodaného tovaru nezodpovedajú špecifikácií tovaru uvedenej v prílohe č. 1 tejto zmluvy.

Dodaný tovar musí byť zhodný s jeho špecifikáciou v prílohe č. 1 tejto zmluvy, ktorá je obsahom zhodná so špecifikáciou tovaru uvedenou v ponuke predloženej predávajúcim vo verejnom obstarávaní.

9. Zaškolenie zamestnancov kupujúceho o obsluhu a údržbe tovaru je predávajúci povinný realizovať najneskôr pri uvedení tovaru do prevádzky v mieste dodania. O zaškolení spíšu zmluvné strany Protokol o zaškolení, s uvedením menného zoznamu zaškolených osôb; zaškolenie potvrdzujú zaškolené osoby svojim podpisom na protokole o zaškolení.
10. Predávajúci je povinný spolu s tovarom dodať kupujúcemu aj príslušnú dokumentáciu k tovaru.
11. Kupujúci je povinný, najneskôr ku dňu dodania tovaru a služieb do miesta dodania, pripraviť miesto dodania tak, aby predávajúci mohol riadne a včas nainštalovať, odskúšať a uviesť tovar do prevádzky.
12. Plnú funkčnosť predmetu zmluvy potvrdí predávajúci a kupujúci písomne a to podpísaním akceptačného protokolu do 5 pracovných dní odo dňa protokolárneho odovzdania predmetu plnenia. Osobou oprávnenou na potvrdenie akceptačného protokolu a potvrdenia funkčnosti za kupujúceho je vedúci zamestnanec Odboru informačných a komunikačných technológií, alebo ním poverený zamestnanec Odboru informačných a komunikačných technológií, e-mail adresa: vagas@unlp.sk, tel. č: +421 !
13. Predávajúci sa zaväzuje pri dodaní tovaru podľa tejto zmluvy povinný predložiť kupujúcemu zoznam a Kontaktné údaje na Klientske pracovisko predávajúceho - tzv. „Hotline“, „Helpdesk“, „Call centrum...“ v zmysle ustanovení tejto zmluvy. Zoznam servisných a kontaktných stredísk predávajúceho tvoria prílohu č. 4 tejto zmluvy.
14. Splnením dodávky predávajúcim sa rozumie dodanie tovaru a súvisiacich služieb v súlade s bodom 12. tohto článku.

Čl. V. Doba platnosti zmluvy

1. Zmluva sa uzatvára na dobu určitú t.j. na jeden obchodný prípad, odo dňa účinnosti tejto zmluvy do doby splnenia dodávky podľa čl. IV. bod 14. tejto zmluvy, okrem ustanovení tejto zmluvy, ktoré upravujú právne vzťahy zmluvných strán aj splnení dodávky podľa čl. IV. bod 14. tejto zmluvy.
2. Táto kúpna zmluva nadobúda platnosť dňom jej podpisu obidvoma zmluvnými stranami a účinnosť dňom nasledujúcim po dne jej zverejnenia v Centrálnom registri zmlúv.
3. Zmluvný vzťah založený touto zmluvou je možné ukončiť:
 - a) písomnou dohodou zmluvných strán,
 - b) odstúpením od zmluvy z dôvodov uvedených v zákone alebo tejto zmluve.
4. Odstúpenie je účinné dňom doručenia písomného oznámenia o odstúpení od zmluvy druhej zmluvnej strane. V prípade pochybností sa má za to, že oznámenie o odstúpení bolo doručené na tretí deň odo dňa jeho zaslania poštou doporučené na adresu sídla druhej zmluvnej strany, pričom deň odoslania sa do tejto lehoty nepočíta.
5. Kupujúci je oprávnený od zmluvy odstúpiť z nasledovných dôvodov:
 - a) ak predávajúci nedodá tovar v súlade s touto zmluvou (čl. IV. bod 14. tejto zmluvy),
 - b) ak kupujúci po dodaní tovaru alebo po predložení príslušnej dokumentácie k tovaru nadobudne dôvodnú pochybnosť o tom, že tovar zodpovedá špecifikácií uvedenej v prílohe č. 1 tejto zmluvy alebo dôvodnú pochybnosť o dôveryhodnosti, správnosti alebo pravdivosti predloženej príslušnej dokumentácii k tovaru,
 - c) ak predávajúci podľa ustanovení tejto zmluvy poruší zmluvu podstatným spôsobom,
 - d) ak predávajúci písomne oznámi, že nie je schopný dodať tovar za podmienok uvedených v tejto zmluve alebo z akéhokoľvek dôvodu tovar podľa tejto zmluvy nedodá,
 - e) ak ponuka predávajúceho predložená vo verejnom obstarávaní bola kupujúcim vyhodnotená ako úspešná v dôsledku preukázateľne vykonaných machinácií a podvodných postupov predávajúceho,
 - f) dôjde k výmazu predávajúceho ako partnera verejného sektora z registra partnerov verejného sektora počas platnosti tejto zmluvy,

- g) ak bolo v súvislosti s výkonom kontroly verejného obstarávania Vykonávateľom, ktorý poskytuje prostriedky mechanizmu, Národnou implementačnou a koordinačnou autoritou (NIKA), Úradom pre verejné obstarávanie, orgánom auditu, prípadne iným obdobným orgánom konštatované porušenie zákona o verejnom obstarávaní alebo iného právneho predpisu, a to bez možnosti predávajúceho uplatniť akékoľvek sankcie voči kupujúcemu,
- h) ak príslušný orgán štátnej správy/ministerstvo, ktoré má ako poskytovateľ finančných prostriedkov realizovať jej financovanie neposkytol finančné prostriedky z akéhokoľvek dôvodu alebo bez uvedenia dôvodu na realizáciu tejto zákazky alebo už poskytnuté finančné prostriedky na realizáciu tejto zákazky verejnému obstarávateľovi – kupujúcemu odňal,
- i) ak výsledky administratívnej kontroly verejného obstarávania neumožňujú financovanie výdavkov vzniknutých z obstarávania predmetu zmluvy alebo kupujúci nesúhlasí s výškou finančnej opravy alebo nesplnil podmienky na uplatnenie finančnej opravy podľa Zmluvy o poskytnutí prostriedkov.

Zmluvné strany sa dohodli, že v prípade odstúpenia kupujúceho od zmluvy z dôvodov, ktoré sú uvedené v ods. h) a i) tohto článku, nevzniká žiadnej zo zmluvných strán nárok na akékoľvek finančné plnenie, majetkové sankcie ani náhradu škody.

Čl. VI. Kúpna cena a platobné podmienky

1. Kúpna cena tovaru je stanovená vzájomnou dohodou zmluvných strán podľa zákona č. 18/1996 Z. z. o cenách, v znení neskorších predpisov, takto :
Kúpna cena za dodaný tovar podľa tejto zmluvy je 236.000,00 € bez DPH, slovom: dvestotridsaťšesť tisíc eur. K uvedenej kúpnej cene sa pripočítava DPH v zákonom stanovenej sadzbe.
Cena jednotlivých položiek dodaného tovaru, vrátane príslušenstva k tovaru a súvisiacich služieb je uvedená v **prílohe č. 2** tejto zmluvy
2. Kúpna cena podľa tohto článku je cenou za nový, kompletný a funkčne bezchybný tovar v minulosti neregistrovaný u iného užívateľa. V uvedenej celkovej kúpnej cene podľa bodu 1. tohto článku je zahrnuté: cena tovaru, clo, dopravné náklady, náklady na inštaláciu a uvedenie do prevádzky, zaškolenie zamestnancov o obsluhu a údržbe tovaru, príslušná dokumentácia, opravy, servis a údržba tovaru, vrátane náhradných dielov a ďalších nákladov s tým spojených počas celej záručnej doby a všetky ostatné finančné náklady spojené s dodaním tovaru kupujúcemu.
3. Právo na zaplatenie celkovej kúpnej ceny vzniká predávajúcemu riadnym splnením jeho záväzkov spôsobom uvedeným v čl. IV. bod 14. tejto zmluvy.
Kupujúci je povinný uhradiť kúpnu cenu za tovar podľa tohto článku na základe faktúry vystavenej predávajúcim bezhotovostným bankovým prevodom na účet predávajúceho podľa čl. I. bod 1. tejto zmluvy.
4. Lehota splatnosti faktúry je 60 kalendárnych dní odo dňa doručenia faktúry kupujúcemu.
5. Predávajúci je povinný vystaviť faktúru kupujúcemu do 15 dní od dňa dodania tovaru podľa čl. IV. bod 14. tejto zmluvy, najneskôr však do piateho pracovného dňa v mesiaci nasledujúceho po mesiaci, v ktorom bol tovar dodaný. Faktúra musí obsahovať náležitosti podľa platných právnych predpisov SR v čase fakturácie. V prípade, že doručená faktúra nebude vystavená správne, je kupujúci oprávnený predmetnú faktúru vrátiť predávajúcemu. Predávajúci je povinný vystaviť novú faktúru a doručiť ju kupujúcemu.
6. Vlastnícke právo k tovaru nadobudne kupujúci až úplným zaplatením celkovej kúpnej ceny podľa tohto článku.
7. Za deň úhrady celkovej kúpnej ceny sa považuje deň jej pripísania na účet predávajúceho.

Čl. VII. Reklamácia tovaru, vady tovaru

1. Pre dodaný predmet plnenia poskytne predávajúci kupujúcemu záruku v trvaní 60 mesiacov. Táto záručná doba začína plynúť odo dňa riadneho splnenia dodávky podľa čl. IV. bod 14. tejto zmluvy.
2. Dodaný predmet plnenia musí v rámci záručnej doby poskytovať plnú funkčnosť a prevádzkovú kontinuitu a to bez dodatočných finančných nákladov na licencie, aktualizácie a technickú podporu.
3. Predávajúci ručí za vlastnosti tovaru počas záručnej doby (podľa bodu 1. tohto článku) vrátane aktualizácií licencií, technickej podpory ako aj iných nevyhnutných súčastí zabezpečujúcich správnu a bezpečnú prevádzku predmetu plnenia.
4. Záruka na predmet dodania podľa tohto článku platí za predpokladu, že kupujúci tovar používa a obsluhuje s príslušnou starostlivosťou podľa inštrukcií obsiahnutých v príslušnej dokumentácii tovaru.
5. Predávajúci neručí za vady spôsobené nesprávnou manipuláciou a obsluhou zamestnancami kupujúceho. Záruka sa predlžuje automaticky o dobu, po ktorú predmet zmluvy nemohol byť v záručnej dobe plne používaný z dôvodu vady.
6. Kupujúci sa zaväzuje že vady (poruchy) ohlásí bezodkladne po ich zistení. Ohlásenie vady za kupujúceho oznámi predávajúcemu oprávnená osoba kupujúceho. Osobou oprávnenou za kupujúceho reklamovať predmet zmluvy a žiadať odstránenie vady počas záručnej doby je vedúci zamestnanec Odboru informačných a komunikačných technológií alebo ním poverený zamestnanec.
7. V záručnej dobe je predávajúci povinný bezplatne odstrániť všetky vady dodaného tovaru.
8. Zmluvné strany sa dohodli, že v prípade vady tovaru počas záručnej doby, má kupujúci právo požadovať a predávajúceho povinnosť bezplatne odstrániť vady tovaru a poradenskú starostlivosť.
9. Predávajúci sa zaväzuje v rámci trvania 60 mesačnej záručnej doby vzťahujúcej sa na tovar podľa tejto zmluvy poskytnúť pre kupujúceho servisnú podporu.
10. Technická telefonická podpora pri riešení vady/chyby inf. systému/zariadenia bude poskytovaná predávajúcim v pracovnom čase 08:00 - 17:00 hod., v pracovných dňoch (9/ 5 business days) prostredníctvom svojho klientskeho pracoviska, pričom predávajúci musí garantovať funkčnosť a prevádzku tohto klientskeho pracoviska. Kupujúci zároveň požaduje, aby predávajúci zabezpečil okrem telefonickej podpory možnosť nahlásenia vady/chyby na zariadení (servisnej udalosti) prostredníctvom webu a/alebo mobilnej aplikácie výrobcu pre iOS aj Android (tzv. HelpDesk) s možnosťou nahlásenia servisnej udalosti dvadsaťštyri (24) hodín denne a sedem (7) dní v týždni.
HelpDesk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:
L1 podpory IS (Level 1, priamy kontakt zákazníka)
L2 podpory IS (Level 2, postúpenie požiadaviek od L1)
L3 podpory IS (Level 3, postúpenie požiadaviek od L2) - zabezpečuje úspešný uchádzač.

Riešenie vád/chýb – SLA parametre.

Za vadu/chybu je považované správanie sa inf. systému/zariadenia v rozpore s prevádzkovou a používateľskou dokumentáciou.

Vady/chyby (prevádzkové problémy) sa podľa závažnosti a požadovaných časov reakcie a ich vyriešenia členia do týchto kategórií:

Kategória A - vysoká - vážne prevádzkové problémy navodzujúce stav, keď nie je možné vykonať hlavné úkony a to i na úrovni prehliadania dát a kupujúci nie je schopný rutinne plniť svoje úlohy. Jedná sa o stav, keď je priamo ohrozená funkcia systému/zariadenia, alebo je nevyhnutné pristúpiť ku komplikovaným a nákladným spôsobom riešenia mimo systému/zariadenia.

Reakčná doba od nahlásenia problému: do 4 hod.

Doba konečného vyriešenia problému od nahlásenia (DKVP): max. do 24 hod. nasledujúci pracovný deň.

Kategória B - stredná - chyby a nedostatky, ktoré spôsobia čiastočné obmedzenie používania systému, avšak činnosť systému/zariadenia je možné podľa pokynov Predávajúceho dočasne nahradiť inou funkcionalitou, i keď za cenu vyššej prácnosti.

Reakčná doba od nahlásenia problému: do 24 hod.

Doba konečného vyriešenia problému od nahlásenia (DKVP): max. do 48 hod. nasledujúci pracovný deň.

Kategória C - nízka - nezávažné prevádzkové chyby, keď niektorá z funkcionalít systému/zariadenia nie je úplne funkčná, ale tento stav má len zanedbateľný dopad na prevádzku Kupujúceho, alebo také, ktoré nie sú uvedené kategóriách A alebo B.

Reakčná doba od nahlásenia problému: do 72 hod.

Doba konečného vyriešenia problému od nahlásenia (DKVP): Vyriešenie a nasadenie v rámci plánovaných aktualizácií systému/zariadenia alebo dohodou.

11. Predávajúci je povinný zabezpečiť vlastný systém na nahlásenie väd v režime 24 hodín 7 týždni s centrálnou adresou monitorovania podpory tzv. „helpdesk“. Kontaktné údaje dodávateľa v súvislosti s týmto bodom, sú uvedené v **Prílohe č.4.** tejto zmluvy.
Pre plnenie tohto bodu je kupujúci povinný zabezpečiť možnosť vzdialeného pripojenia predávajúceho do prostredia kupujúceho.
12. Predávajúci sa zaväzuje zabezpečiť prostriedky pre automatizované vytváranie servisných požiadaviek z prostredia kupujúceho v prípade vzniku vady systému.
13. Kupujúci požaduje možnosť bezplatného sťahovania updatov firmvérov a ovládačov aj po uplynutí doby servisnej podpory HW výrobcu.
14. Zmluvné strany sa dohodli, že v prípade vady tovaru počas záručnej doby, má kupujúci právo požadovať a predávajúci povinnosť bezplatne odstrániť vady tovaru, vrátane, nie však len, všetkých prác spojených s opravami tovaru, dodávky náhradných dielov nutných k bezchybnému prevádzkovaniu tovaru, poradenskej starostlivosti o inštalovaný tovar, dodávky funkčného príslušenstva k tovaru, ktorého nefunkčnosť nie je zavinená kupujúcim.
15. Predávajúci neručí za vady spôsobené nesprávnou manipuláciou a obsluhou zamestnancami kupujúceho. Záruka sa predlžuje automaticky o dobu, po ktorú predmet plnenia nemohol byť v záručnej dobe plne používaný z dôvodu poruchy alebo vady.
16. Kupujúci sa zaväzuje že vady (poruchy) tovaru uplatní bezodkladne po ich zistení. Ohlásenie vady tovaru za kupujúceho oznámi predávajúcemu oprávnená osoba kupujúceho. Osobou oprávnenou za kupujúceho reklamovať tovar a žiadať odstránenie vady počas záručnej doby je vedúci zamestnanec Odboru informačných a komunikačných technológií alebo ním poverený zamestnanec , e-mail adresa: vagas@unlp.sk , tel. č.+421 !
17. Kupujúci je povinný vady tovaru nahlásiť predávajúcemu písomne na e-mail adresu : sales@smartsectechnologies.sk ,alebo kontaktovať jedno z kontaktných stredísk Predávajúceho uvedených v Prílohe č. 4 tejto zmluvy.
18. Predávajúci je povinný zabezpečovať autorizovaný záručný servis t.j. opravy a servis tovaru len odborne kvalifikovanými osobami.

Čl. VIII. Majetkové sankcie

1. V prípade nedodržania podmienok plnenia uvedených v čl. IV. bod 1 tejto zmluvy zo strany predávajúceho je kupujúci oprávnený vyúčtovať a predávajúci je povinný zaplatiť za každý jednotlivý prípad porušenia zmluvných podmienok zmluvnú pokutu vo výške 1 000,- €, slovom: jedentisíc eur. Zmluvná pokuta je splatná v lehote do 30 kalendárnych dní odo dňa doručenia faktúry predávajúcemu.
2. V prípade omeškania s úhradou faktúry je predávajúci oprávnený uplatniť si nárok na zaplatenie úroku z omeškania vo výške podľa platných právnych predpisov SR. Úroky z omeškania sú splatné v lehote do 30 kalendárnych dní odo dňa doručenia faktúry kupujúcemu.
3. Zmluvné strany sa dohodli, že v prípade, ak predávajúci poruší povinnosti uvedené v čl. IX. bod 2. a/alebo 3. tejto zmluvy je povinný uhradiť kupujúcemu zmluvnú pokutu vo výške 10 % z kúpnej ceny bez DPH , ktorá ako pohľadávka bola predmetom postúpenia alebo iného

právneho úkonu, ktorým došlo k zmene v osobe veriteľa. Zmluvná pokuta je splatná v lehote do 30 kalendárnych dní odo dňa doručenia faktúry predávajúcemu.

4. Uplatnením majetkových sankcií podľa tohto článku nie je dotknuté právo poškodenej zmluvnej strany na náhradu škody.
5. Zmluvné strany sa dohodli, že v prípade, ak predávajúci poruší povinnosti uvedené v čl. X bod 1. tejto Zmluvy je povinný uhradiť kupujúcemu zmluvnú pokutu vo výške 1 000,- €, slovom: jedentisíc eur. Zmluvná pokuta je splatná v lehote do 30 kalendárnych dní odo dňa doručenia faktúry predávajúcemu.

Čl. IX. Osobitné ustanovenia

1. Zmluvné strany sa zaväzujú oznámiť druhej zmluvnej strane všetky zmeny údajov dôležitých pre bezproblémové plnenie zmluvy.
2. Zmluvné strany sa dohodli, že pohľadávku, ktorá vznikne z tohto zmluvného vzťahu predávajúcemu ako veriteľovi, predávajúci nepostúpi tretej osobe bez predchádzajúceho písomného súhlasu kupujúceho ako dlžníka. Písomný súhlas za kupujúceho je oprávnený vydať len jeho štatutárny orgán. Postúpenie pohľadávok predávajúcim bez predchádzajúceho písomného súhlasu kupujúceho je neplatné s odkazom na § 525 ods. 2 zák. č. 40/1964 Zb. Občiansky zákonník, v znení neskorších predpisov. Porušenie povinností uvedené v tomto bode je považované za závažné porušenie tejto zmluvy.
3. Predávajúci sa zaväzuje, že nevykoná bez predchádzajúceho písomného súhlasu kupujúceho ako dlžníka, žiadny právny úkon, ktorým by bola alebo ktorého dôsledkom by bola alebo mohla byť zmena v osobe predávajúceho ako veriteľa, ktorý mu umožňuje platná právna úprava o zabezpečení záväzku, najmä nie však výlučne, pohľadávku nezaloží ako majetok, neprijme ponuku ručenia alebo bankovej záruky, nepristúpi k dohode o započítaní pohľadávok so svojim veriteľom a to vo vzťahu k pohľadávkam, vrátane príslušenstva, ktoré ku dňu platnosti tejto zmluvy existujú a ktoré v budúcnosti vzniknú z ich akéhokoľvek vzájomného zmluvného vzťahu predávajúcemu ako veriteľovi a kupujúcemu ako dlžníkovi. Zmluvné strany sa dohodli, že akýkoľvek právny úkon predávajúceho ako veriteľa vedúci k zmene v osobe veriteľa je bez predchádzajúceho písomného súhlasu kupujúceho ako dlžníka absolútne neplatný. Súhlas za kupujúceho je oprávnený vydať len jeho štatutárny orgán. Porušenie povinností uvedené v tomto bode je považované za závažné porušenie tejto zmluvy.
4. Predávajúci sa zaväzuje, že
 - a) nevyužije akékoľvek informácie, ktoré zistí alebo s prihliadnutím na okolnosti by mohol zistiť pri plnení predmetu tejto zmluvy vo svoj prospech, ani v prospech tretích osôb, počas trvania tohto zmluvného vzťahu, a ani po ukončení platnosti tejto Zmluvy;
 - b) všetky informácie a písomné dokumenty, ktoré budú na základe tejto Zmluvy vypracované, bude považovať za dôverné, a to bez časového obmedzenia aj po ukončení platnosti tejto Zmluvy;
 - c) informácie a podklady poskytnuté kupujúcim alebo tretími osobami pre plnenie predmetu tejto Zmluvy nepoužije na iný účel ako je plnenie tejto Zmluvy;
 - d) bude zachovávať mlčanlivosť o všetkých informáciách získaných v súvislosti s touto zmluvou alebo získaných pri plnení tejto zmluvy a tieto informácie nebude zverejňovať, ani žiadnym spôsobom rozširovať.
5. Predávajúci nie je oprávnený previesť alebo postúpiť práva a povinnosti z tejto zmluvy tretej osobe bez predchádzajúceho písomného súhlasu kupujúceho. Postúpenie práv a povinností bez predchádzajúceho písomného súhlasu kupujúceho je neplatné. Súhlas kupujúceho je platný len za podmienky, ak bol na takýto právny úkon udelený predchádzajúci písomný súhlas zriaďovateľa kupujúceho t. j. Ministerstvo zdravotníctva SR.
6. Predávajúci je povinný, v zmysle zák. č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zabezpečiť ochranu osobných údajov osôb, ktoré kupujúci pri svojej činnosti spracúva a s ktorými môže prísť predávajúci, zamestnanci predávajúceho a tretie osoby vo vzťahu k predávajúcemu, do styku pri vykonávaní činnosti podľa tejto zmluvy.

Predávajúci je povinný poučiť o povinnosti mlčanlivosti zamestnancov predávajúceho a všetky tretie osoby, ktoré v mene predávajúceho budú vykonávať činnosti alebo sa akýmkoľvek spôsobom budú zúčastňovať na plnení tejto zmluvy predávajúcim.

7. Predávajúci sa zaväzuje strpieť výkon kontroly/audit/ v súvislosti s plnením tejto zmluvy kedykoľvek počas platnosti **Zmluvy o poskytnutí prostriedkov**, oprávnenými osobami na výkon kontroly/audit/ a poskytnúť týmto osobám riadne a včas všetku potrebnú súčinnosť. Porušenie povinnosti uvedenej v tomto bode je považované za porušenie zmluvy podstatným spôsobom. Oprávnenými osobami sú oprávnené osoby podľa **Zmluvy o poskytnutí prostriedkov**.
8. Kontaktná osoba predávajúceho pre účely plnenia tejto zmluvy je: Jozef Dobiš, tel. kontakt: 0905 708650, e-mail adresa: jd@smartsectechnologies.sk
9. Kontaktná osoba kupujúceho pre účely plnenia tejto zmluvy je vedúci Odboru informačných a komunikačných technológií, e-mail adresa: vagas@unlp.sk, tel.č. tel. č.+421 ! alebo ním určený zamestnanec.
10. Predávajúci berie na vedomie a akceptuje že:
 - a) kupujúci zverejní túto zmluvu (ako aj jej dodatky) ako povinne zverejňovanú zmluvu v Centrálnom registri zmlúv vedenom Úradom vlády SR v súlade so zák.č. 546/2010 Z.z.,
 - b) predmet plnenia tejto zmluvy bude financovaný kupujúcim aj prostredníctvom prostriedkov mechanizmu na podporu obnovy a odolnosti podľa čl. II. bod 5. tejto zmluvy,
 - c) na plnenie tejto zmluvy sa vzťahujú ustanovenia **Zmluvy o poskytnutí prostriedkov** uvedenej v čl. II. bod 5. tejto zmluvy a predávajúci zároveň prehlasuje, že sa s obsahom vyššie uvedenej zmluvy oboznámi a zaväzuje sa plniť jej podmienky v postavení predávajúceho vzťahujúce sa na alebo v súvislosti s plnením tejto zmluvy.
11. Predávajúci vyhlasuje, že v prípade, ak mu v súvislosti s uzatvorením tejto zmluvy vznikla povinnosť byť zapísaný v registri partnerov verejného sektora v zmysle zákona č. 315/2016 Z.z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (ďalej len „ZorPVS“), je ku dňu uzatvorenia tejto zmluvy zapísaný v registri partnerov verejného sektora, ktorého správnom a prevádzkovateľom je MS SR. Ak sa na subdodávateľov predávajúceho (čl. X. tejto zmluvy) vzťahuje povinnosť byť zapísaný v registri partnerov verejného sektora v zmysle ZorPVS, predávajúci je povinný zabezpečiť plnenie tejto povinnosti všetkými subdodávateľmi. V prípade, ak počas plnenia tejto zmluvy dôjde k právoplatnému výmazu niektorého zo subdodávateľov v registri partnerov verejného sektora, je predávajúci povinný bezodkladne ukončiť plnenie tejto zmluvy prostredníctvom tohto subdodávateľa.

Čl. X. Subdodávky

1. Predávajúci je oprávnený zabezpečiť časť plnenia predmetu tejto Zmluvy prostredníctvom svojich subdodávateľov, pričom subdodávateľ musí spĺňať podmienky účasti subdodávateľa uvedené vo verejnom obstarávaní a zároveň predávajúci :
 - a) je povinný plnenie tejto zmluvy zadať len subdodávateľovi uvedenému v Prílohe č. 3 tejto Zmluvy s rozsahom jeho plnenia uvedeným vo verejnom obstarávaní;
 - b) garantuje spôsobilosť každého zo subdodávateľov uvedených v prílohe č. 3 tejto Zmluvy, pre plnenie predmetu tejto Zmluvy;
 - c) zodpovedá za celé a riadne plnenie tejto Zmluvy počas celej doby platnosti tejto Zmluvy a to bez ohľadu na to, či Predávajúci použil na plnenie predmetu tejto Zmluvy subdodávky alebo nie, v akom rozsahu a za akých podmienok. Kupujúci nenesie žiadnu zodpovednosť a nemá žiadne povinnosti vyplývajúce z tejto Zmluvy voči subdodávateľom Predávajúceho.
 - d) je povinný v prípade zmeny subdodávateľa alebo v prípade doplnenia nového subdodávateľa vo vzťahu k plneniu, ktorého sa táto Zmluva týka písomne oznámiť Kupujúcemu akúkoľvek zmenu údajov o subdodávateľovi a to do piatich pracovných dní odo dňa, kedy táto skutočnosť nastala;
 - e) je povinný do piatich pracovných dní odo dňa uzatvorenia zmluvy so subdodávateľom predložiť Kupujúcemu aktualizovaný zoznam subdodávateľov, ktorý musí obsahovať minimálne identifikáciu subdodávateľa, predmet a presný rozsah subdodávky,

predpokladaný podiel plnenia zadávaný subdodávateľovi vo vzťahu k celému rozsahu plnenia a osobu oprávnenú konať za subdodávateľa (meno a priezvisko, adresa pobytu, dátum narodenia); Zoznam subdodávateľov je uvedený Prílohe č. 3 tejto Zmluvy. Na zmenu v zozname subdodávateľov t. j. zmenu Prílohy č. 3 tejto Zmluvy sa vyžaduje uzatvorenie dodatku k tejto Zmluve.

2. Predávajúci zodpovedá za plnenie tejto Zmluvy alebo jej časti subdodávateľom, akoby plnenie Zmluvy vykonal sám/osobne.
3. Porušenie povinností Predávajúceho uvedených v tomto článku Zmluvy sa považuje za podstatné porušenie tejto Zmluvy.

Čl. XI. Záverečné ustanovenia

1. Meniť a dopĺňať túto zmluvu je možné len na základe dohody oboch zmluvných strán a to vo forme písomného dodatku. Dodatok k tejto zmluve nesmie byť uzatvorený v rozpore s ust. zák. č. 343/2015 Z. z. .
2. Právne vzťahy neupravené touto zmluvou sa riadia najmä príslušnými ustanoveniami zák. č. 513/1991 Zb. Obchodný zákonník, v znení neskorších predpisov a ďalšími súvisiaci právnymi predpismi SR.
3. Zmluva je vyhotovená v štyroch vyhotoveniach, z ktorých dve vyhotovenia obdrží predávajúci a dve vyhotovenia kupujúci.
4. Neoddeliteľnou súčasťou zmluvy sú:
Príloha č. 1 - Špecifikácia tovaru
Príloha č. 2 - Kalkulácia ceny
Príloha č. 3 - Zoznam subdodávateľov
Príloha č. 4 - Zoznam kontaktných a servisných stredísk predávajúceho
Príloha č. 5 - Protikorupčná doložka
Príloha č. 6 - Zmluva o zabezpečení plnenia bezp. opatrení a notifikačných povinností

V Košiciach, dňa
Kupujúci :

V Bratislave , dňa
Predávajúci:

MUDr. Ľuboslav Beňa, PhD., MPH
Riaditeľ
Univerzitná nemocnica L. Pasteura Košice

Ing. Jozef Dobiš, konateľ
SmartSec Technologies s.r.o.

Príloha č. 1 Špecifikácia tovaru

1. Palo Alto Networks, FW PA-3410, Precision AI Network Subscription Bundle, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN, 5 years term
2. Virtual systems upgrade- Additional 10 virtual systems (1 to 11) for PA-3410
3. Partner enabled premium support 5 year term, PA-3410
4. Palo Alto Networks PA-3410 with redundant AC power supplies
5. Palo Alto Networks PA-3400 Series 4 post rack mount kit
6. Power cord for Continental Europe with IEC-60320 C13 and CEE 7/ SCHUKO cords ends, 10A, 250Vmax, Gft
7. PA-3410 Device Security subscription, 5 years term
8. Implementation

Príloha č. 2 Kalkulácia ceny

1. Palo Alto Networks, FW PA-3410, Precision AI Network Subscription Bundle, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN, 5 years term
2. Virtual systems upgrade- Additional 10 virtual systems (1 to 11) for PA-3410
3. Partner enabled premium support 5 year term, PA-3410
4. Palo Alto Networks PA-3410 with redundant AC power supplies
5. Palo Alto Networks PA-3400 Series 4 post rack mount kit
6. Power cord for Continental Europe with IEC-60320 C13 and CEE 7/ SCHUKO cords ends, 10A, 250Vmax, 6ft
7. PA-3410 Device Security subscription, 5 years term
8. Implementation

Cena celkom za implementáciu, HW, SW a support na 5 rokov je 236.000,00 Euro bez DPH.

Ing. Jozef Dobiš, konteľ
SmartSec Technologies s.r.o
Dňa:

Príloha č. 3 Subdodávateľa

Subdodávateľ č. 1. *:

a/	Obchodné meno	Aricoma a.s.
b/	Sídlo	Krasovského 14, 851 01 Bratislava
c/	IČO	36396222
d/	Predmet subdodávky	Implementácia
e/	Presný rozsah subdodávky	Inštalácia, implementácia do WAN/LAN
f/	Percentuálny podiel tejto subdodávky z celkového plnenia zmluvy	11
g/	Osoba oprávnená konať za subdodávateľa	Meno a priezvisko : Mario Háronik Funkcia: konateľ Tel. kontakt: E-mail adresa :
h/	Iné	

Subdodávateľ č. 2. *:

a/	Obchodné meno	
b/	Sídlo	
c/	IČO	
d/	Predmet subdodávky	
e/	Presný rozsah subdodávky	
f/	Percentuálny podiel tejto subdodávky z celkového plnenia zmluvy	
g/	Osoba oprávnená konať za subdodávateľa	Meno a priezvisko : Funkcia: Tel. kontakt: E-mail adresa :
h/	Iné	

* Pokiaľ predávajúci bude zabezpečovať plnenie tejto zmluvy prostredníctvom svojich subdodávateľov (čl. X. tejto zmluvy) vpíše všetky požadované údaje do tabuliek vyššie.

**V prípade, že predávajúci plnenie tejto zmluvy nebude zabezpečovať prostredníctvom svojich subdodávateľov (čl. X. tejto zmluvy) preškrtnie vyššie uvedené tabuľky a túto skutočnosť potvrdí podpisom prehlásenia na tejto prílohe:

Prehlásenie predávajúceho **:

Predávajúci týmto prehlasuje, že plnenie tejto zmluvy nebude zabezpečovať prostredníctvom svojich subdodávateľov (čl. X. tejto zmluvy).

V Bratislave dňa

Predávajúci :

Príloha č. 4 Zoznam kontaktných a servisných stredísk

BRATISLAVA

Einsteinova Business Center, Krasovského 14, Bratislava, 851 01

Tel.: +421

E-mail:

Otváracia doba: Po - Pia: 8:00 - 17:00

ŽILINA

Bratislavská 29, Žilina, 010 01

Tel.: +421

E-mail:

Otváracia doba: Po - Pia: 8:00 - 16:30

KOŠICE

Bardejovská 1/C, Košice, 040 11

Tel.: +421

E-mail:

Otváracia doba: Po - Pia: 7:30 - 16:30

BANSKÁ BYSTRICA

Rudlovská cesta 64, Banská Bystrica, 974 11

Tel.: +421

E-mail:

Otváracia doba: Po - Pia: 8:00 - 16:30

TRENČÍN

Bratislavská 853, Trenčín, 911 05

Tel.: +421

E-mail: :

Otváracia doba: Po - Pia: 8:00 - 16:00

PREŠOV

Prostějovská 127/D, Prešov, 080 01

Tel.: +421

E-mail: :

Otváracia doba: Po - Pia: 7:30 - 12:00, 13:00 - 16:00

SERVICEDESK

Tel.: :

E-mail: :

Príloha č. 5 Protikorupčná doložka

1. SYSTÉM RIADENIA

Strana zmluvného vzťahu sa zaväzuje, že v rámci svojej organizácie prijme účinný systém riadenia schopný zabrániť korupčným trestným činom úplatkárstva/podplácania s cieľom zneužitia úradnej moci, právomoci, vplyvu či postavenia, za účelom porušenia zákona, úplatkárstva pri právnych úkonoch, navádzania na takéto zneužitie, vydieranie a/alebo spreneveru.

2. PLATOBNÉ SYSTÉMY

Strana zmluvného vzťahu sa pri výkone činností v rámci zmluvného vzťahu so spoločnosťou Univerzitná nemocnica L. Pasteura Košice (ďalej len „UNLP“) zaväzuje:

- a) vykonávať platby výhradne takým spôsobom, ktorý umožňuje identifikáciu príjemcu,
- b) vyhýbať sa hotovostným platbám alebo platbám v naturáliách.

3. DARY A ODMENY

Strana zmluvného vzťahu sa zaväzuje, že žiaden z jej predstaviteľov, zástupcov, zamestnancov, alebo iných osôb konajúcich v jeho mene pred uzatvorením alebo počas plynutia zmluvného vzťahu nebude priamo alebo nepriamo ponúkať, dávať, poskytovať, vyžadovať ani prijímať finančné prostriedky alebo akékoľvek iné oceneľné hodnoty, alebo poskytovať akékoľvek výhody, dary, alebo pohostenia za účelom ovplyvňovať konanie UNLP, s využitím odmeňovania, alebo navádzania k nekorektnému výkonu príslušných predstaviteľov UNLP za účelom získania alebo udržania výhody pri výkone jej činnosti v rozpore so všeobecne záväznými právnymi predpismi Slovenskej republiky (ďalej len „SR“). Je možné však poskytnúť prejav zdvorilosti s nízkou finančnou hodnotou napr. knihy, kvety, katalógy, drobné spomienkové predmety pri pracovných stretnutiach alebo oficiálnych rokovaníach.

4. VZŤAH K POLITICKÝM STRANÁM ALEBO K VEREJNÝM ORGANIZÁCIÁM

Strana zmluvného vzťahu nesmie vyvíjať či už priamy alebo nepriamy nátlak na politických predstaviteľov, zamestnancov štátnej a verejnej správy (napríklad poskytovaním vlastných priestorov, prijímaním navrhnutých uchádzačov o prácu, konzultovaním dohôd) s cieľom získať výhody pri uzatváraní zmluvných vzťahov s UNLP.

5. NULOVÝ KONFLIKT ZÁUJMOV

Strana zmluvného vzťahu vyhlasuje, že žiaden z jej štatutárnych zástupcov:

- a) nevykonáva, ani nevykonával činnosti, ktoré by predstavovali konflikt záujmov z hľadiska uzatvorenia zmluvného vzťahu s UNLP,
- b) nebol trestne stíhaný za:
 - subvenčný podvod,
 - skresľovanie údajov hospodárskej a obchodnej evidencie (uviedenie nepravdivých alebo hrubo skresľujúcich údajov alebo zatajenie povinných údajov o závažných skutočnostiach vo výkazoch),
 - korupciu (§ 328 – 336 zákona č. 300/2005 Z.z. Trestný zákon v znení neskorších predpisov; napr.: Prijímanie úplatku, Podplácanie, Nepriamu korupciu).

6. KLAUZULA PROTI ÚPLATKÁRSTVU

Strana zmluvného vzťahu požiadavky UNLP uvedené v tejto doložke, vyplývajúce z platných právnych predpisov Slovenskej republiky v rámci boja proti korupcii berie na vedomie a zaväzuje sa k ich dodržiavaniu. V prípade potreby bližšie špecifikovať požiadavky tejto proti korupčnej doložky, bude UNLP akceptovať znenie schváleného Proti korupčného programu u konkrétnej strany zmluvného vzťahu .

Zároveň sa zaväzuje okamžite oznámiť primeranou formou určenému zástupcovi UNLP, akékoľvek podozrenie na porušenie ktoréhokoľvek ustanovenia tejto doložky, a byť plne súčinný pri dôkladnom šetrení podozrenia.

Ak UNLP preukáže partnerovi zmluvného vzťahu porušenie akéhokoľvek ustanovenia tejto doložky:

- a) je oprávnená pozastaviť plnenie predmetu zmluvného vzťahu po predchádzajúcom písomnom upozornení, a to po dobu, ktorú považuje za nevyhnutnú vzhľadom na rozsah a charakter zistenia, maximálne však na dobu jedného mesiaca. Strana zmluvného vzťahu berie na vedomie a súhlasí, že počas doby nevyhnutnej na zisťovanie skutočností pre vyšetrovanie podozrenia na porušenie ustanovení tejto doložky nebudú vznikať akékoľvek povinnosti a/alebo sankcie voči UNLP, vyplývajúce z takéhoto pozastaveného plnenia zmluvného vzťahu,
- b) strana zmluvného vzťahu je povinná prijať všetky relevantné opatrenia, aby zabránila strate, zneužitiu alebo zničeniu listinných a iných dôkazov vzťahujúcich sa k príslušnému konaniu.

Príloha č. 6 Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Samostatná príloha zmluvy

**Príloha č. 6 Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
(ďalej aj ako „zmluva“)**

podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení
neskorších predpisov
uzatvorená medzi

1. Kupujúci: Univerzitná nemocnica L. Pasteura Košice

so sídlom: Rastislavova 43, 041 01 Košice
v zastúpení: MUDr. Ľuboslav Beňa, PhD., MPH, riaditeľ
IČO: 00606707
DIČ: 2021141969
IČ DPH: SK2021141969
Zriadená Zriaďovacou listinou MZ SR č. 1842/1990 – A/I-2 zo dňa 18.12.1990

(ďalej len „Kupujúci“)

2. Predávajúci: SmartSec Technologies s.r.o.

so sídlom: Jágeho 6, Bratislava 821 08
v zastúpení: Ing. Jozef Dobiš, konateľ
IČO: 50448676
DIČ: 2120361452
IČ DPH: SK2120361452

(ďalej len „Predávajúci“)

(ďalej spolu ako „zmluvné strany“)

Čl. I. Úvodné ustanovenia

1. Kupujúci je v zmysle Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**ZoKB**“) Prevádzkovateľom základnej služby. Predávajúci berie na vedomie, že uzatvára zmluvu s poskytovateľom kritickej základnej služby v zmysle § 18 ZoKB.
2. Predávajúci uzatvára s Kupujúcim kúpnu zmluvu č. 18827/2025 (ďalej len „**hlavná zmluva**“), ktorej predmet priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Kupujúceho.
3. Kupujúci je ako prevádzkovateľ základnej služby v zmysle § 19 ods. 2 ZoKB povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Kupujúceho prostredníctvom tretej strany, uzatvoriť s treťou stranou – Predávajúcim zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa ZoKB počas celej doby výkonu tejto činnosti (ďalej aj ako „**bezpečnostná zmluva**“), ktorú týmto uzatvára.
4. Predávajúci vyhlasuje, že disponuje technickým, technologickým a personálnym vybavením, ktoré je potrebné na plnenie požiadaviek vyplývajúcich z bezpečnostnej zmluvy, a že má zavedené úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy.
5. Predávajúci je povinný v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zabezpečiť ochranu osobných údajov osôb, ktoré Kupujúci pri svojej činnosti spracúva a s ktorými môže prísť Predávajúci, zamestnanci Predávajúceho a tretie osoby vo vzťahu k Predávajúcemu do styku pri vykonávaní činnosti podľa tejto zmluvy. Predávajúci je povinný poučiť o povinnosti mlčanlivosti zamestnancov Predávajúceho a všetky tretie osoby, ktoré v mene Predávajúceho budú vykonávať činnosti alebo sa akýmkoľvek spôsobom budú zúčastňovať na plnení tejto zmluvy Predávajúcim.
6. Predávajúci prehlasuje, že spôsob a rozsah spracovania osobných údajov je v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a je dodržaný princíp minimalizácie spracovania osobných údajov pre daný účel. Ak je možné rozsah spracovávaných osobných údajov ešte viac minimalizovať, je Predávajúci povinný daný proces okamžite zabezpečiť.

7. Predávajúci sa zaväzuje informovať Kupujúceho o všetkých tretích stranách, ktorým majú byť poskytnuté informácie za účelom plnenia tejto zmluvy.
8. Zrušenie bezpečnostnej zmluvy nemá vplyv na povinnosť Predávajúceho zachovávať mlčanlivosť a ochranu informácií.

Čl. II. Predmet zmluvy

1. Predmetom tejto bezpečnostnej zmluvy (Prílohy č. 6 hlavnej zmluvy) je stanovenie základných podmienok a princípov spolupráce Zmluvných strán vrátane určenia práv a povinností Zmluvných strán pri plnení bezpečnostných opatrení, notifikačných povinností a súvisiacich náležitostí realizovaných v nadväznosti na hlavnú zmluvu, a to najmä určenie záväzku Predávajúceho ako tretej osoby zabezpečiť kybernetickú bezpečnosť dodávaných služieb pre prevádzkovaný informačný systém dodávaný Predávajúcim podľa hlavnej zmluvy.
2. Bezpečnostné opatrenia a notifikačné povinnosti v rozsahu stanovenom v tejto bezpečnostnej zmluve sa Predávajúci zaväzuje plniť od okamihu nadobudnutia účinnosti hlavnej zmluvy až do skončenia účinnosti hlavnej zmluvy, s výnimkou tých povinností Predávajúceho, ktoré majú ostať v zmysle osobitných právnych predpisov platné a účinné i po skončení účinnosti hlavnej zmluvy.

Čl. III. Obdobie trvania zmluvy

Táto bezpečnostná zmluva sa uzatvára na dobu platnosti a účinnosti hlavnej zmluvy.

Čl. IV. Povinnosť Predávajúceho dodržiavať bezpečnostnú politiku Kupujúceho

1. Predávajúci sa pri realizácii zmluvnej činnosti vyplývajúcej z hlavnej zmluvy zaväzuje dodržiavať platnú bezpečnostnú politiku Kupujúceho, t. j. platnú a účinnú riadiacu dokumentáciu Kupujúceho v oblasti kybernetickej bezpečnosti, s ktorou ho Kupujúci neodkladne oboznámi.
2. Predávajúci podpisom tejto zmluvy vyjadruje súhlas s bezpečnostnou politikou Kupujúceho.
3. Predávajúci je povinný a zaväzuje sa chrániť všetky informácie, ktoré mu Kupujúci v súvislosti s plnením zmluvy poskytol.

Čl. V. Špecifikácia a rozsah bezpečnostných opatrení

Predávajúci prijíma vo vlastnej spoločnosti bezpečnostné opatrenia minimálne v nasledovných oblastiach:

1. Správa zraniteľností a kybernetických hrozieb (§ 20 ods. 2 písm. b) ZoKB).
Cieľom opatrenia je odhaliť zraniteľnosti informačných systémov a zariadení skôr než bude zneužitá a prerastie do bezpečnostného incidentu.
2. Riadenie udalostí a kybernetických bezpečnostných incidentov (§ 20 ods. 2 písm. d) ZoKB).
Cieľom opatrenia je detegovať a riešiť kybernetické bezpečnostné incidenty, ktoré môžu mať negatívny dopad na výkon činnosti pre Kupujúceho.
3. Správa identít a prístupov (§ 20 ods. 2 písm. j) ZoKB).
Cieľom opatrenia je jednoznačná identifikácia prístupu osôb k sieti a informačným systémom.
4. Bezpečnosť pri prevádzke sietí a informačných systémov (§ 20 ods. 2 písm. k) ZoKB).
Cieľom opatrenia je zabrániť útočníkovi prístupu k jednotlivým sieťam a informačným systémom ako aj pohybu medzi nimi.
5. Ochranu proti škodlivému kódu a nežiaducemu obsahu (§ 20 ods. 2 písm. l) ZoKB).
Cieľom opatrenia je ochrana pred následkami zneužitia škodlivého kódu útočníkom.
6. Monitorovanie, zaznamenávanie a hlásenie udalostí (§ 20 ods. 2 písm. n) ZoKB).
Cieľom opatrenia je predchádzanie bezpečnostným incidentom a zlepšovanie bezpečnostných opatrení.

Čl. VI. Rozsah činnosti Predávajúceho

Predávajúci bude realizovať zmluvné činnosti v rozsahu podľa:

- predmetu hlavnej zmluvy
- príloh, ktoré sú súčasťou hlavnej zmluvy

Čl. VII. Riadenie bezpečnostných incidentov

1. Predávajúci a Kupujúci (ďalej aj ako „zmluvné strany“) sa zaväzujú, že upovedomia druhú zmluvnú stranu o vzniku bezpečnostného incidentu a stupňa závažnosti, alebo bezpečnostnej udalosti spojenej s predmetom tejto

zmluvy bez zbytočného odkladu po tom, ako sa o takomto porušení dozvedeli. Zmluvné strany sú povinné oznámiť vznik bezpečnostného incidentu zaslaním hlásenia o kybernetickom bezpečnostnom incidente (ďalej ako „KBI“) na e-mailovú adresu:

- a) Kupujúci: incident@unlp.sk
 - b) Predávajúci: support@smartsectechnologies.sk
2. Hlásenie musí obsahovať minimálne:
 - a) Informácie o tom, kto hlási KBI
 - b) Informácie o KBI v rozsahu potrebnom na jeho riadnu identifikáciu
 - c) Informácie o službe zasiahnutej KBI
 3. Zmluvné strany sa zaväzujú riešiť KBI odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „reaktívne opatrenie“).
 4. Pri riešení KBI sú zmluvné strany povinné na žiadosť druhej zmluvnej strany spolupracovať s Národným bezpečnostným úradom a Ministerstvom zdravotníctva Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
 5. Predávajúci sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok (digitálnu stopu) tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Kupujúcemu.
 6. Predávajúci sa zaväzuje oznámiť Kupujúcemu skutočnosť, že v súvislosti s KBI mohlo dôjsť k spáchaniu trestného činu.
 7. Predávajúci sa zaväzuje bezodkladne oznámiť a preukázať Kupujúcemu vykonanie reaktívneho opatrenia a jeho výsledok.
 8. Po vyriešení KBI je Predávajúci na výzvu Kupujúceho v určenej lehote povinný predložiť Kupujúcemu návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu bezpečnostného incidentu (ďalej len „ochranné opatrenia“) na schválenie.
 9. Ak Predávajúci nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Predávajúci povinný spolupracovať s Kupujúcim na jeho návrhu.
 10. Po schválení ochranného opatrenia Kupujúcim je Predávajúci povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia Predávajúcim, je Predávajúci povinný preveriť jeho účinnosť.

Čl. VIII. Spolupráca zmluvných strán

1. Zmluvné strany sú povinné informovať sa navzájom o všetkých skutočnostiach, dôležitých pre plnenie tejto zmluvy.
2. Kupujúci je povinný z legislatívnych a technologických dôvodov akceptovať vývoj systému/zariadenia. Inštaláciu aktuálneho upgradu systému môže odmietnuť iba zo závažných dôvodov, na nevyhnutnú dobu a len po vzájomnej dohode s Predávajúcim.
3. Kupujúci sa zaväzuje prijímať priebežne také opatrenia, aby bol systém/zariadenie prevádzkované v prostredí odpovedajúcom definovaným systémovým požiadavkám.
4. Zmluvné strany sú povinné vytvoriť a udržiavať zoznam osôb, prístupujúcich na základe plnenia tejto zmluvy k systému/zariadeniu s administrátorskými právami.
5. V prípade, ak Predávajúci využíva pre výkon činností definovaných touto zmluvou aj subdodávateľov, zodpovedá za ochranu informácií, kvalitu, bezpečnosť a včasnosť služieb rovnako, ako keby danú činnosť realizoval sám.
6. Predávajúci je povinný oboznámiť subdodávateľov o požiadavkách na informačnú bezpečnosť a bezpečnostných pravidlách, ktorú sú povinní dodržiavať pri výkone danej činnosti.
7. Predávajúci poučí svojich zamestnancov a zamestnancov subdodávateľov a všetky osoby, ktoré v rámci poskytovania služieb v zmysle tejto zmluvy majú prístup k informáciám Kupujúceho, a to najmä s dôrazom na povinnosť mlčanlivosti a sankciami za porušenie tejto mlčanlivosti. Každá osoba Predávajúceho, zúčastnená

na predmete plnenia, vlastnoručne podpisuje vyjadrenie o zachovaní mlčanlivosti podľa par. 12 ods. 1 ZoKB. Predávajúci sa zaväzuje zabezpečiť a odovzdať Kupujúcemu tieto písomné vyjadrenia o zachovávaní mlčanlivosti.

8. Predávajúci bude poskytovať svoje služby osobne alebo vzdialeným pripojením. Pre prípad potreby poskytovať služby osobne (fyzicky v prostredí Kupujúceho) je Predávajúci povinný o plánovanej návšteve vopred oboznámiť Kupujúceho. Zhotoviteľ sa nesmie pohybovať v chránených a prísne chránených zónach Kupujúceho bez prítomnosti zodpovednej osoby Kupujúceho.

Pre vzdialený prístup do prostredia Kupujúceho musí mať zamestnanec Predávajúceho vygenerovaný VPN prístup s jednoznačnou identifikáciou Predávajúceho. Zriadenie vzdialeného prístupu (VPN) zabezpečuje odbor informačných a komunikačných technológií Kupujúceho (e-mail: informatika@unlp.sk).

V prípade zmeny v zozname zamestnancov Predávajúceho, je Predávajúci povinný každú zmenu v personálnom obsadení oznámiť Kupujúcemu e-mailom na adresu: mkb@unlp.sk v lehote do dvoch pracovných dní odo dňa účinnosti personálnej zmeny.

Zoznam zamestnancov Predávajúceho, ktorí budú poskytovať služby Kupujúcemu:

Meno a priezvisko	Pracovná pozícia/rola	E-mail	Tel. kontakt	Forma prístupu (osobne/vzdialene)
Jozef Dobiš	riadiť			Osobne/vzdialene
Michal Grega	MKB			Osobne/vzdialene

Čl. IX. Auditné činnosti u Predávajúceho

1. Kupujúci si vyhradzuje právo realizovať u Predávajúceho auditné činnosti za účelom priebežnej kontroly bezpečnostných požiadaviek Kupujúceho súvisiacich s predmetom plnenia tejto zmluvy.
2. Kupujúci je oprávnený vykonať u Predávajúceho auditné činnosti, zamerané na overenie plnenia povinností Predávajúceho podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Predávajúceho na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Predávajúceho pre plnenie cieľov tejto zmluvy.
3. Rozsah auditných činností musí byť adekvátny rozsahu služieb poskytovaných touto zmluvou a nesmie zasahovať do práv a zmluvných záväzkov Predávajúceho.
4. Kupujúci môže uvedené auditné činnosti u Predávajúceho realizovať sám alebo prostredníctvom tretej osoby ktorá musí byť kompetentná a mať oprávnenie pre výkon auditných činností.
5. Kupujúci sa zaväzuje oznámiť Predávajúcemu najmenej 30 (tridsať) pracovných dní vopred svoj zámer realizovať u Predávajúceho auditné činnosti.
6. Kupujúci sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditných činností, a ktoré nie sú verejne známe.

Čl. X. Podmienky a spôsob ukončenia zmluvy

1. Zmluvné strany môžu túto bezpečnostnú zmluvu ukončiť vždy písomnou dohodou zmluvných strán; Bezpečnostná zmluva zaniká dňom dohodnutým v písomnom vyhotovení dohody o ukončení tejto bezpečnostnej zmluvy, nikdy nie pred uplynutím účinnosti hlavnej zmluvy s Kupujúcim. V prípade, ak zmluvné strany dohodnú deň ukončenia bezpečnostnej zmluvy pred dňom uplynutia účinnosti hlavnej zmluvy, táto bezpečnostná zmluva zaniká súčasne so zánikom účinnosti hlavnej zmluvy.
2. Kupujúci je oprávnený písomne odstúpiť od tejto bezpečnostnej zmluvy v prípade, ak Predávajúci porušuje svoje povinnosti vyplývajúce z tejto Zmluvy:
 - a) Predávajúci neodôvodnene odmietne výkon auditnej činnosti Kupujúcim,
 - b) Predávajúci postúpi svoje práva a povinnosti na ďalšieho Predávajúceho v rozpore s touto zmluvou,

- c) na majetok Predávajúceho je vyhlásený konkurz, exekúcia, Predávajúci vstúpil do likvidácie, preruší, alebo iným spôsobom ukončí svoju podnikateľskú činnosť,
 - d) Predávajúci, alebo osoba oprávnená konať v jeho mene je právoplatne odsúdená za trestný čin spáchaný v súvislosti s výkonom jeho činnosti, alebo s podnikaním,
 - e) Predávajúci stratí predpoklady na plnenie tejto zmluvy.
3. Výpovedná lehota je jeden mesiac a začína plynúť prvého dňa mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.
4. Predávajúci je povinný po ukončení hlavnej zmluvy vrátiť, previesť alebo rozhodnutím Kupujúceho zničiť všetky informácie, ku ktorým mal ako tretia strana počas trvania zmluvného vzťahu prístup.
5. Predávajúci je povinný po ukončení zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovej základnej služby na Kupujúceho; tento záväzok Predávajúceho ostáva v platnosti aj po ukončení zmluvy po dobu 5 rokov.

Čl. XI. Sankcie, zmluvné pokuty a náhrada škody

3. V prípade, ak Predávajúci poruší svoje povinnosti v zmysle tejto zmluvy voči Kupujúcemu, a to najmä povinnosť:
- a) dodržiavať bezpečnostné politiky Kupujúceho,
 - b) prijímať a dodržiavať bezpečnostné opatrenia minimálne v rozsahu špecifikovanom v Článku V. tejto zmluvy,
 - c) umožniť Kupujúcemu vykonať audit bezpečnostných opatrení prijatých Predávajúcim, a to najmä za účelom zistenia súladu/nesúladu prijatých bezpečnostných opatrení Predávajúcim s bezpečnostnou politikou Kupujúceho,
 - d) oznámiť Kupujúcemu každú zmenu v personálnom obsadení (personálne zmeny v zozname pracovných rolí), a to v lehote do dvoch pracovných dní od účinnosti personálnej zmeny,
 - e) zabezpečiť a odovzdať Kupujúcemu písomné vyjadrenie o zachovávaní mlčanlivosti každej osoby zúčastnenej na predmete plnenia,
- vzniká Kupujúcemu nárok na zaplatenie zmluvnej pokuty vo výške 10.000,- EUR (slovom: desať tisíc eur).
4. Kupujúci je oprávnený uplatniť si zmluvné pokuty a náhradu škody kedykoľvek v priebehu plnenia predmetu zmluvy, ako aj po zániku zmluvy v prípade, ak porušenie zmluvných podmienok stanovených touto zmluvou zistí po zániku zmluvného vzťahu vyplývajúceho zo zmluvy.
5. V prípade, ak Predávajúci poruší svoje povinnosti podľa čl. X. bod 5. tejto zmluvy, vzniká Kupujúcemu nárok na zaplatenie zmluvnej pokuty vo výške 50.000,- EUR (slovom: päťdesiat tisíc eur).
6. Uplatnením ktorejkoľvek zmluvnej pokuty alebo zmluvných pokút v zmysle tohto článku nie je dotknutý nárok Kupujúceho na náhradu vzniknutej škody v celom rozsahu a právo na uplatnenie ďalšej zmluvnej pokuty podľa tejto zmluvy. Kupujúci môže uplatňovať náhradu škody a zmluvnej pokuty kumulatívne, Kupujúci má nárok na zaplatenie zmluvnej pokuty a súčasne náhrady škody v plnom rozsahu. Kupujúci je oprávnený jednostranne započítať voči Predávajúcemu svoje pohľadávky vzniknuté z titulu zmluvnej pokuty a/alebo náhrady škody uplatnenej podľa tejto zmluvy.

Názov predmetu zákazky:

Technológie sieťovej a komunikačnej bezpečnosti

ČESTNÉ VYHLÁSENIE UCHÁDZAČA

k splneniu podmienky účasti podľa § 32 ods. 1 písm. a) ZVO v nadväznosti na § 32 ods. 7 a 8 ZVO

Obchodný názov uchádzača: SmartSec Technologies s.r.o.

V zastúpení: Ing. Jozef Dobiš, konateľ

Sídlo uchádzača: Jégeho 6, Bratislava 821 08

IČO: 50448676

DIČ: 2120361452

- V zmysle § 32 ods. 1 písm. a) ZVO podmienku účasti musí spĺňať aj iná osoba ako osoba podľa § 32 ods. 1 písm. a) ZVO, ak táto osoba má právo za ňu konať, práva spojené s rozhodovaním alebo kontrolou v hospodárskom subjekte, ktorý sa chce zúčastniť verejného obstarávania
- Za takúto osobu sa považuje osoba, ktorá má rozhodujúci vplyv na činnosť uchádzača alebo záujemcu, jeho strategické ciele alebo významné rozhodnutia prostredníctvom vlastníckeho práva, finančného podielu alebo pravidiel, ktorými sa uchádzač alebo záujemca spravuje, pričom rozhodujúcim vplyvom sa rozumie, ak iná osoba
- a) vlastní väčšinu akcií alebo väčšinový obchodný podiel u uchádzača alebo záujemcu,
 - b) má väčšinu hlasovacích práv u uchádzača alebo záujemcu,
 - c) má právo vymenúvať alebo odvolávať väčšinu členov štatutárneho orgánu alebo dozorného orgánu uchádzača alebo záujemcu alebo
 - d) má právo vykonávať rozhodujúci vplyv na základe dohody uzavretej s uchádzačom alebo záujemcom alebo na základe spoločenskej zmluvy, zakladateľskej listiny alebo stanov, ak to umožňuje právo štátu, ktorými sa táto osoba riadi.
- Splnenie podmienky účasti preukazuje uchádzač alebo záujemca verejnemu obstarávateľovi predložením čestného vyhlásenia alebo vyhlásenia podľa § 32 ods. 5 ZVO, ak právo štátu uchádzača alebo záujemcu so sídlom, miestom podnikania alebo obvyklým pobytom mimo územia Slovenskej republiky neupravuje inštitút čestného vyhlásenia, ako súčasť ponuky.

V súvislosti s uvedeným verejným obstarávaním a na vyššie uvedené účely, predkladám toto čestné vyhlásenie aj s uvedením zoznamu osôb podľa § 32 ods. 7 a 8 ZVO a **čestne vyhlasujem**, že nižšie uvedené osoby spĺňajú podmienku účasti podľa § 32 ods. 1 písm. a) ZVO

Identifikácia osôb podľa § 32 ods. 7 a 8 ZVO: ÁNO/NIE* (v prípade, ak uchádzač označí možnosť nie, nižšie uvedené údaje nevyplní)

Titul, meno, priezvisko, funkcia

V Bratislave, dňa

meno, priezvisko, funkcia oprávnenej osoby
podpis a pečiatka

Ing. Jozef Dobiš

Zmluva o spolupráci

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení
neskorších predpisov
(ďalej len „Zmluva“)

medzi zmluvnými stranami

Objednávateľom: **SmartSec Technologies s.r.o.**
Sídlo: Jégeho 6, 821 08 Bratislava, Slovenská republika
Štatutárny orgán: Ing. Jozef Dobiš, konateľ
IČO: 50448676
DIČ: 2120361452
IČ DPH: SK2120361452
Bankové spojenie: Tatrabanka a.s.
EUR IBAN: SK7611000000002947028013
Zapísaný: OR Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 114228/B

ďalej ako „objednávateľ“

a

Poskytovateľom: **Aricoma Systems s.r.o.**
Sídlo: Krasovského 14, 851 01 Bratislava, Slovenská republika
Štatutárny orgán: Mário Háronik, konateľ
IČO: 36396222
DIČ: 2020105428
IČ DPH: SK2020105428
Bankové spojenie: Slovenská sporiteľňa, a. s.
EUR IBAN: SK53 0900 0000 0050 3080 8601, SWIFT: GIBASKBX
Zapísaný: OR Mestského súdu Bratislava III, Oddiel: Sro, Vložka číslo: 130357/B

ďalej aj „poskytovateľ“

1. PREDMET ZMLUVY

- 1.1. Objednávateľ sa rozhodol, že sa samostatne zúčastní verejného obstarávania, vyhláseného verejným obstarávateľom Univerzitná nemocnica L. Pasteura Košice, IČO: 00606707 (ďalej aj len „verejný obstarávateľ“), uverejnenom vo Vestníku č. 174/2025 dňa 28.08.2025 pod zn. 14025 - MST na predmet zákazky s názvom „Technológie sieťovej a komunikačnej bezpečnosti“, referenčné číslo: UNLP-2025-83-NZ-VS (ďalej len „VO“) a v súlade s ust. § 34 ods. 3 zákona č. 343/2015 Z. z. Zákona o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“) využije technické a odborné kapacity inej osoby (poskytovateľa) na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti
- 1.2. Predmetom tejto Zmluvy je dohoda o spôsobe a podmienkach spolupráce zmluvných strán v súvislosti s prípravou ponuky a účasťou spoločnosti SmartSec Technologies s.r.o. vo VO, ako aj s realizáciou zákazky v prípade, ak bude ponuka spoločnosti SmartSec Technologies s.r.o. vo VO úspešná.
- 1.3. Poskytovateľ sa zaväzuje poskytnúť pre objednávateľa technické a odborné kapacity na účely preukázania splnenia podmienok účasti objednávateľa inou osobu v oblasti technickej alebo odbornej spôsobilosti objednávateľa, uvedené v súťažných podkladoch v časti B, ods. 3 *PODMIENKY ÚČASTI UCHÁDZAČOV VO VEREJNOM*

OBSTARÁVANÍ TÝKAJÚCE SA TECHNICKEJ SPÔSOBILOSTI ALEBO ODBORNEJ SPÔSOBILOSTI.

- zoznamom dodávok tovaru za predchádzajúce tri roky podľa § 34 ods. 1 písm. a) ZVO
 - 2 certifikovaný špecialisti na úrovni minimálne PROFESSIONAL na firewallovú technológiu
 - 1 certifikovanú osobu projektového manažéra
- 1.4. Poskytovateľ sa zaväzuje spolupracovať s objednávatelom počas celého trvania zmluvného vzťahu medzi objednávatelom a verejným obstarávateľom na vyššie uvedenom predmet zákazky za predpokladu, ak sa objednávatel stane víťazom VO a uzavrie s verejným obstarávateľom zmluvu na realizáciu predmetu VO.
- 1.5. Poskytovateľ vyhlasuje, že spĺňa podmienky účasti vo Verejnom obstarávaní podľa ust. § 32 ods. 1 Zákona o verejnom obstarávaní – Osobné postavenie a neexistujú u neho dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až h) a ods. 7 ZVO, čo preukazuje:
- a) Informáciou, že spoločnosť Aricoma Systems s.r.o. je zapísaná v registri hospodárskych subjektov vedeným Úradom pre verejné obstarávanie pod registračným číslom 2023/2-PO-F2179

<https://www.uvo.gov.sk/>

2. PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

- 2.1. Pri plnení predmetu tejto Zmluvy sa poskytovateľ zaväzuje, že bude:
- postupovať s náležitou odbornou starostlivosťou,
 - uskutočňovať činnosť, na ktorú sa touto Zmluvou zaviazal, a to podľa pokynov objednávatel'a,
 - oznamovať objednávatel'ovi informácie, ktoré sú dôležité pre jeho rozhodovanie,
 - vystupovať tak, aby neohrozil dobré meno a povesť objednávatel'a,
 - upozorňovať objednávatel'a na možné ťažkosti pri plnení jeho povinností a vynaložiť všetko úsilie na ich odstránenie.
- 2.2. Poskytovateľ má právo požadovať od objednávatel'a súčinnosť potrebnú na splnenie svojich záväzkov.
- 2.3. Poskytovateľ má právo na riadne a včasné zaplatenie dohodnutej odmeny.
- 2.4. Objednávatel' má právo na včasné a riadne splnenie predmetu zmluvy podľa tejto Zmluvy.
- 2.5. Objednávatel' je povinný včas poskytnúť poskytovateľ'ovi pokyny, písomnosti, informácie a iné veci, ktoré sú potrebné na splnenie predmetu zmluvy podľa tejto Zmluvy a poskytnúť mu aj inú potrebnú súčinnosť (ďalej aj len „súčinnosť“), ak je táto vzhľadom na svoju povahu obvyklá, alebo potrebná za účelom riadneho splnenia predmetu plnenia.
- 2.6. Objednávatel' je povinný písomne upozorniť poskytovateľ'a na možné ťažkosti pri plnení zmluvných povinností a vynaložiť všetko úsilie na ich odstránenie
- 2.7. Objednávatel' je povinný riadne a včas platiť dojednanú odmenu.
- 2.8. Poskytovateľ v súvislosti s uzatvorením tejto Zmluvy poskytuje Objednávatel'ovi osobné údaje svojich zamestnancov (ďalej len „osobné údaje“), pričom sa Objednávatel' zaväzuje tieto osobné údaje spracúvať v pozícii prevádzkovateľa v

súlade s ustanoveniami zákona č. 18/2018 Z. z. o ochrane osobných údajov a Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR).

- 2.9. Objednávateľ je povinný zachovávať mlčanlivosť o osobných údajoch, nezverejňovať ich tretím osobám, okrem Obstarávateľa a zaväzuje sa spracúvať osobné údaje výlučne za účelom splnenia podmienok jeho účasti vo VO a plnenia predmetu zákazky VO.
- 2.10. Objednávateľ informuje Poskytovateľa, že ním poskytnuté osobné údaje zamestnancov Poskytovateľa poskytne verejnému obstarávateľovi vo VO v zmysle čl. 13 ods. 3 Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR).

3. PLATNOSŤ ZMLUVY

- 3.1. Táto Zmluva sa uzatvára na dobu platnosti a účinnosti zmluvy, ktorá by vznikla medzi SmartSec Technologies s.r.o. a verejným obstarávateľom na základe tohto VO za predpokladu, ak sa objednávateľ stane víťazom VO.
- 3.2. Ak zmluvný vzťah medzi SmartSec Technologies s.r.o. a verejným obstarávateľom vôbec nevznikne, Zmluva zanikne konečným rozhodnutím VO alebo odvolacieho orgánu, z ktorého bude zrejmé, že ponuka spoločnosti SmartSec Technologies s.r.o. nie je vo VO úspešná.

4. OBCHODNÉ TAJOMSTVO

- 4.1. Všetky skutočnosti súvisiace s právnym vzťahom založeným touto Zmluvou budú zmluvné strany považovať za prísne dôverné skutočnosti. Ktorákoľvek zo zmluvných strán nesmie predmetné dôverné skutočnosti oznámiť, sprístupniť alebo využiť pre seba alebo pre iného bez predchádzajúceho písomného súhlasu druhej zmluvnej strany. Za porušenie tohto článku sa nepovažuje zverejnenie druhej zmluvnej strany ako referencie ani prípadné povinné sprístupnenie a/alebo zverejnenie zmluvy podľa zákona č. 546/2010 Z. z. a súvisiacich osobitných predpisov v platnom znení.
- 4.2. Na obchodné tajomstvo zmluvných strán sa vzťahuje § 17 a nasl. Obchodného zákonníka.

5. ZÁVEREČNÉ USTANOVENIA

- 5.1. Táto Zmluva nadobúda platnosť a účinnosť dňom jej podpisu obidvom zmluvnými stranami.
- 5.2. Vzájomné vzťahy zmluvných strán vyplývajúce z tejto zmluvy sa riadia právnym poriadkom Slovenskej republiky.
- 5.3. Práva a povinnosti zmluvných strán, ktoré nie sú výslovne upravené v tejto Zmluve, sa riadia príslušnými ustanoveniami Obchodného zákonníka (zákon č.513/1991 Zb. v znení neskorších predpisov) a iných všeobecne záväzných právnych predpisov Slovenskej republiky.
- 5.4. Zmluvné strany vyhlasujú, že si túto Zmluvu pred jej podpisom prečítali, jej obsahu porozumeli a na potvrdenie toho, že obsah tejto Zmluvy zodpovedá ich skutočnej a slobodnej vôli, ju vlastnoručne podpísali.
- 5.5. Táto Zmluva je vyhotovená v elektronickej podobe a podpísaná kvalifikovanými elektronickými podpismi oprávnených osôb zmluvných strán. Zmluva je určená pre každú zmluvnú stranu a jeden rovnopis pre účely preukázania splnenia podmienok účasti vo VO.

Za poskytovateľa:

Aricoma Systems s.r.o.

Žilina dňa:

.....
Mario Háronik

konateľ konateľ

Za objednávateľa:

SmartSec Technologies s.r.o.

Bratislava dňa:

.....
Ing. Jozef Dobiš

ČESTNÉ VYHLÁSENIE

Aricoma Systems s.r.o., so sídlom Krasovského 14, Bratislava - mestská časť Petržalka 851 01, Slovenská republika, IČO: 36 396 222, spoločnosť zapísaná v Obchodnom registri vedenom Mestským súdom Bratislava III, oddiel Sro., vložka č.130357/B (ďalej aj ako „Spoločnosť“), v mene ktorej koná Mario Hároník, konateľ

čestne vyhlasuje, že

osoba v zmysle ustanovenia § 32 ods. 7 a ods. 8 zákona č. 343/2015 Z.z o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj ako „ZVO“), ktorou je spoločnosť:

Aricoma Systems a.s., sídlo Hornopolská 3322/34, Moravská Ostrava, 702 00 Ostrava, IČO: 043 08 697, Česká republika, spoločnosť zapísaná v Obchodnom registri vedenom Krajským súdom v Brne, oddiel B, vložka č. 11012

ako aj osoby v zmysle ustanovenia § 32 ods. 1 písm. a) ZVO, t.j.

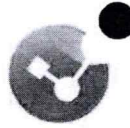
- členovia jej štatutárneho orgánu – predstavenstva:
 - Predseda predstavenstva Milan Sameš, dat.nar. ČR
 - člen predstavenstva Tomáš Ječmínek, dat. nar. , ČR
 - podpredseda predstavenstva Kristína Šmída , dat. nar. , ČR
 - člen predstavenstva Vít Ševčík, dat. nar. , ČR
 - člen predstavenstva Jaroslav Dvořák, dat. nar. , ČR
- členovia jej dozorného orgánu - dozornej rady:
 - predseda dozornej rady David Emr, dat. nar. , ČR
 - člen dozornej rady Vlastimil Palata, dat. nar. , ČR
 - člen dozornej rady Hana Zipserová, dat. nar. ČR
- funkcia prokuristov nie je v uvedenej spoločnosti vytvorená

neboli právoplatne odsúdené za trestný čin korupcie, trestný čin poškodzovania finančných záujmov Európskych spoločností, trestný čin legalizácie príjmu z trestnej činnosti, trestný čin založenia, zosnovania a podporovania zločineckej skupiny, trestný čin založenia, zosnovania alebo podporovania teroristickej skupiny, trestný čin terorizmu a niektorých foriem účasti na terorizme, trestný čin obchodovania s ľuďmi, trestný čin, ktorého skutková podstata súvisí s podnikaním alebo trestný čin machinácie pri verejnom obstarávaní a verejnej dražbe **a spĺňajú podmienky účasti v zmysle § 32 ods.1 ZVO.**

Toto čestné vyhlásenie sa vydáva na účely preukázania splnenia podmienky účasti týkajúcej sa osobného postavenia podľa ust. § 32 ods. 1 písm. a) v spojení s ust. § 32 ods. 7 a ods. 8 ZVO.

V Žiline dňa (viď elektronický podpis)

Mario Hároník, konateľ Aricoma Systems s.r.o.



CHECK POINT™

CHECK POINT SOFTWARE TECHNOLOGIES LTD.



THIS CERTIFIES THAT

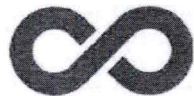
Jozef Burak

HAS DEMONSTRATED THE KNOWLEDGE TO BE A

Check Point Certified Security Master

This 12 day of March 2025

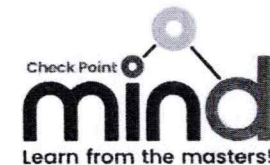
Expiration Date: March 13, 2027



Check Point Infinity
GLOBAL SERVICES

Eitan Lugassi

Vice President, Infinity Global Services



Validate this certificate's authenticity at www.credly.com/org/checkpoint/verify



CHECK POINT™

CHECK POINT SOFTWARE TECHNOLOGIES LTD.



THIS CERTIFIES THAT

Jozef Burak

HAS DEMONSTRATED THE KNOWLEDGE TO BE A

Check Point Certified Security Expert R81

This 29 day of July 2024

Expiration Date: July 29, 2027



Check Point Infinity
GLOBAL SERVICES

Eitan Lugassi

Vice President, Infinity Global Services



Validate this certificate's authenticity at www.checkpoint.com/verify



CHECK POINT

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

TOTO JE POTVRDENIE, ŽE Jozef Burak

PREJAVIL DOSTATOČNÉ VEDOMOSTI NA ZÍSKANIE POZÍCIE AKO

Certifikovaný Expert pre Bezpečnosť Check Point R81

V tento deň, 29. júla 2024

Dátum platnosti do: 29. júla 2027



GLOBAL
SERVICES

Eitan Lugassi, čitateľný podpis

Viceprezident, Infinity Global Services

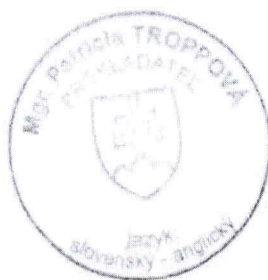
Overte si pravosť certifikátu na stránke www.crediv.com/org/checkpoint/verify

Preklad som vypracovala ako prekladateľka zapísaná v zozname znalcov, tlmočníkov a prekladateľov, ktorý vedie Ministerstvo spravodlivosti Slovenskej republiky v odbore slovenský jazyk - anglický jazyk, evidenčné číslo prekladateľa 970399. Prekladateľský úkon je zapísaný pod poradovým číslom 1395/2005 prekladateľského denníka. Preklad súhlasí s prekladanou listinou.. Som si vedomá právnych dôsledkov v prípade vyhotovenia vedome nepravdivého prekladu.

V Košiciach, dňa:

The translation has been worked out by the translator registered in the List of authorised legal experts, interpreters and translators of the Ministry of Justice of the Slovak Republic in the specialisation for Slovak Language - English Language, registration number of the translator 970399. The translation is registered under the file number 1395/2005 in the Journal of Translations. The translation is accordant to the translated document. I am aware of the legal consequences in case of producing a translation intentionally untrue.

In Košice, date:



PREKLAD Č. 1395 / 2025

ÚRADNÝ PREKLAD Z ANGLICKÉHO JAZYKA DO SLOVENSKEHO JAZYKA

TRANSLATION NO. 1395 / 2025

SWORN TRANSLATION FROM ENGLISH LANGUAGE INTO SLOVAK LANGUAGE

PREKLADATEL / TRANSLATOR: Mgr. Patrícia Troppová

EVIDENČNÉ ČÍSLO / REGISTRATION NUMBER: 970399

ZADÁVATEL / ORDERED BY: Kvalitné preklady, s.r.o.

POČET STRÁN PREKLADU/ NUMBER OF PAGES OF THE TRANSLATION: 1/1

POČET ODOVZDANÝCH VYHOTOVENÍ/NUMBER OF PROVIDED COPIES: 1/1

VYHOTOVENÝ DŇA:/ PRODUCED ON: 18.08.2025



CHECK POINT™

CHECK POINT SOFTWARE TECHNOLOGIES LTD.



THIS CERTIFIES THAT

Richard Vlcek

HAS DEMONSTRATED THE KNOWLEDGE TO BE A

Check Point Certified Security Expert R81

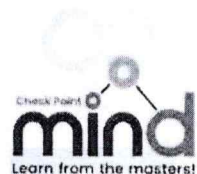
This 29 day of July 2024

Expiration Date: July 29, 2027



Check Point Infinity
GLOBAL SERVICES

Eitan Lugassi
Vice President, Infinity Global Services



Validate this certificate's authenticity at www.credly.com/org/checkpoint/verify



CHECK POINT

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

TOTO JE POTVRDENIE, ŽE Richard Vlcek

PREJAVIL DOSTATOČNÉ VEDOMOSTI NA ZÍSKANIE POZÍCIE AKO

Certifikovaný Expert pre Bezpečnosť Check Point R81

V tento deň, 29. júla 2024

Dátum platnosti do: 29. júla 2027



Eitan Lugassi, čitateľný podpis

Viceprezident, Infinity Global Services



Overte si pravosť certifikátu na stránke www.crediv.com/org/checkpoint/verify

Preklad som vypracovala ako prekladateľka zapísaná v zozname znalcov, tlmočníkov a prekladateľov, ktorý vedie Ministerstvo spravodlivosti Slovenskej republiky v odbore slovenský jazyk - anglický jazyk, evidenčné číslo prekladateľa 970399. Prekladateľský úkon je zapísaný pod poradovým číslom 126/2015 prekladateľského denníka. Preklad súhlasí s prekladanou listinou.. Som si vedomá právnych dôsledkov v prípade vyhotovenia vedome nepravdivého prekladu.

V Košiciach, dňa:

The translation has been worked out by the translator registered in the List of authorised legal experts, interpreters and translators of the Ministry of Justice of the Slovak Republic in the specialisation for Slovak Language - English Language, registration number of the translator 970399. The translation is registered under the file number 126/2015 in the Journal of Translations. The translation is accordant to the translated document. I am aware of the legal consequences in case of producing a translation intentionally untrue.

In Košice, date:





CHECK POINT

CHECK POINT SOFTWARE TECHNOLOGIES LTD.



THIS CERTIFIES THAT

Richard Vlcek

HAS DEMONSTRATED THE KNOWLEDGE TO BE A

Check Point Certified Security Master

This 9 day of April 2025

Expiration Date: April 10, 2027



Check Point Infinity
GLOBAL SERVICES

Eitan Lugassi
Vice President, Infinity Global Services



Validate this certificate's authenticity at www.credly.com/org/checkpoint/verify



CHECK POINT

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

TOTO JE POTVRDENIE, ŽE Richard Vlcek

PREJAVIL DOSTATOČNÉ VEDOMOSTI NA ZÍSKANIE POZÍCIE AKO

Certifikovaný Riaditeľ pre Bezpečnosť Check Point

V tento deň, 9. apríla 2025

Dátum platnosti do: 10. apríla 2027



GLOBAL
SERVICES

Eitan Lugassi, čitateľný podpis

Viceprezident, Infinity Global Services

Overte si pravosť certifikátu na stránke www.crediv.com/org/checkpoint/verify

Preklad som vypracovala ako prekladateľka zapísaná v zozname znalcov, tlmočníkov a prekladateľov, ktorý vedie Ministerstvo spravodlivosti Slovenskej republiky v odbore slovenský jazyk - anglický jazyk, evidenčné číslo prekladateľa 970399. Prekladateľský úkon je zapísaný pod poradovým číslom 1247/1025 prekladateľského denníka. Preklad súhlasí s prekladanou listinou.. Som si vedomá právnych dôsledkov v prípade vyhotovenia vedome nepravdivého prekladu.

V Košiciach, dňa:

The translation has been worked out by the translator registered in the List of authorised legal experts, interpreters and translators of the Ministry of Justice of the Slovak Republic in the specialisation for Slovak Language - English Language, registration number of the translator 970399. The translation is registered under the file number 1247/1025 in the Journal of Translations. The translation is accordant to the translated document. I am aware of the legal consequences in case of producing a translation intentionally untrue.

In Košice, date:



This is to certify that

PETER LAJS

Has achieved the

PRINCE2® Practitioner Certificate in Project Management

Effective from **26 Sep 2014**

Renew by 22 Mar 2027

Certificate number

Candidate number

Byron Nicolaides
Chairman and Group CEO, PeopleCert

PRINCE2 5th-edition

Printed on 22 March 2024

This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.

QJTL QRESILIA QPRINCE2 QPRINCE2
ABLE QAgileSHIFT QMBP QMQR QP30/3 QP30 QMQR QMQR

[illegible]

Toto je potvrdenie, že
PETER LAJS

dosiahol

**Certifikát Practitioner v
oblasti riadenia projektov PRINCE2®**

Platné od **26. 09. 2014**

Obnovenie **22.03. 2027**

Číslo certifikátu

Číslo kandidáta

Nečitateľný podpis
Byron Nicolaides
Predseda predstavenstva a generálny
riaditeľ skupiny, PeopleCert

PRINCE2 5.edícia

Vytlačené 22.3.2024

Toto osvedčenie zostáva majetkom skúšobného ústavu, ktorý ho vydal, a na požiadanie sa okamžite vráti

PREKLAD Č. 1246 / 2025

ÚRADNÝ PREKLAD Z ANGLICKÉHO JAZYKA DO SLOVENSKEHO JAZYKA

TRANSLATION NO. 1246 / 2025

SWORN TRANSLATION FROM ENGLISH LANGUAGE INTO SLOVAK LANGUAGE

PREKLADATEĽ / TRANSLATOR: Mgr. Patrícia Troppová

EVIDENČNÉ ČÍSLO / REGISTRATION NUMBER: 970399

ZADÁVATEĽ / ORDERED BY: Kvalitné preklady, s.r.o.

POČET STRÁN PREKLADU / NUMBER OF PAGES OF THE TRANSLATION: 1/1

POČET ODOVZDANÝCH VYHOTOVENÍ / NUMBER OF PROVIDED COPIES: 1/1

VYHOTOVENÝ DŇA: / PRODUCED ON: 29.07.2025

Preklad som vypracovala ako prekladateľka zapísaná v zozname znalcov, tlmočníkov a prekladateľov, ktorý vedie Ministerstvo spravodlivosti Slovenskej republiky v odbore slovenský jazyk - anglický jazyk, evidenčné číslo prekladateľa 970399. Prekladateľský úkon je zapísaný pod poradovým číslom 341/2025 prekladateľského denníka. Preklad súhlasí s prekladanou listinou. Som si vedomá právnych dôsledkov v prípade vyhotovenia vedome nepravdivého prekladu.

V Košiciach, dňa: _____

The translation has been worked out by the translator registered in the List of authorised legal experts, interpreters and translators of the Ministry of Justice of the Slovak Republic in the specialisation for Slovak Language - English Language, registration number of the translator 970399. The translation is registered under the file number 341/2025 in the Journal of Translations. The translation is accordant to the translated document. I am aware of the legal consequences in case of producing a translation intentionally untrue.

In Košice, date: _____





Declaration of Conformity



Palo Alto Networks declares that under our sole responsibility the following product and all its options:

Model:

PA-3410, PA-3420, PA-3430, PA-3440

is in conformity with the following harmonized standards and fulfill the essential requirements of the LVD Directive 2014/35/EU, EMC Directive 2014/30/EU, WEEE Directive 2012/19/EU, and RoHS Directives 2011/65/EU and 2015/863/EU.

Standards

EN 55032: 2015 +A11:2020
EN 55035: 2017 +A11:2020
EN61000-3-2:2014
EN61000-3-3:2013
EN62368-1:2014+A11:2017

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054-1211
United States of America
408-753-4000

Director, HW Quality Engineering

Mary O'Callaghan

Date: January 24, 2022



PA-3410



PA-3420



PA-3430



PA-3440

PA-3400 Series

Palo Alto Networks PA-3400 Series ML-Powered NGFWs—comprising the PA-3440, PA-3430, PA-3420, and PA-3410—target high-speed internet gateway deployments. The PA-3400 Series appliances secure all traffic.

Highlights

- World's first ML-Powered NGFW
- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls
- Leader in the Forrester Wave: Enterprise Firewalls, Q4 2022
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Native web proxy support in NGFW to simplify and consolidate management of firewall and proxy functionalities
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services
- Supports centralized administration with Panorama® network security management
- Maximizes security investments and prevents business disruptions with Strata™ Cloud Manager

The world's first ML-Powered Next-Generation Firewall (NGFW) enables you to prevent unknown threats, see, and secure everything—including the internet of things (IoT)—and reduce errors with automatic policy recommendations.

The controlling element of the PA-3400 Series is PAN-OS®, the same software that runs all Palo Alto Networks NGFWs. PAN-OS natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The applications, content, and users—the elements that run your business—serve as the basis of your security policies, resulting in an improved security posture and reduced incident response times.

Key Security and Connectivity Features

ML-Powered Next-Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect IoT devices and make policy recommendations; is a cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and Categorizes All Applications, on All Ports, All the Time, with Full Layer 7 Inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (SSL/TLS). In addition, it automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic shaping.
- Offers the ability to create custom App-ID™ tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- Enables safe migration of legacy Layer 4 rule sets to rules based on App-ID with Policy Optimizer built in, giving you a rule set that is more secure and easier to manage.

Check out the [App-ID tech brief](#) for more information.

Enforces Security for User Devices Anywhere While Adapting Policies Based on User Activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android mobile devices; macOS, Windows, and Linux desktops and laptops; Citrix and Microsoft VDI; and terminal servers).

- Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to move quickly toward a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security.

Check out the [Cloud Identity Engine solution brief](#) for more information.

Prevents Malicious Activity Concealed in Encrypted Traffic

- Inspects and applies policy to SSL/TLS-encrypted traffic, both inbound and outbound, including for traffic that uses TLSv1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as the amount of encrypted traffic, SSL/TLS versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly—based on, for example, URL category, source and destination zone, address, user, user group, device, and port—for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).
- Allows you to intelligently forward all traffic (decrypted TLS, undecrypted TLS, and non-TLS) to third-party security tools with a network packet broker and optimize your network performance and reduce operating expenses.

Refer to this [decryption whitepaper](#) to learn where, when, and how to decrypt to prevent threats and secure your business.

Offers AI-Powered Unified Management and Operations with Strata Cloud Manager

- **Prevent network disruptions:** Forecast deployment health and proactively identify capacity bottlenecks up to seven days in advance with predictive analytics to proactively prevent operational disruptions.
- **Strengthen security in real time:** AI-powered analysis of policies and real-time compliance checks against industry and Palo Alto Networks best practices.
- **Enable NetSec management and ops:** Easily manage configuration and security policies across all form factors, including SASE, hardware and software firewalls, and all security services to ensure consistency and reduce operational overhead.

Native Web Proxy Support for the Next-Generation Firewall

- Ability to consolidate firewall and proxy into a single platform while managing capabilities through a centralized management platform to build policies.
- Ability to support explicit proxy through PAC files and also transparent proxy.
- Explicit proxy can help with no-default route architectures with on-premises proxy deployments.
- Explicit proxy supports authentication with Kerberos and SAML.
- Transparent proxy setup is simplified without the need for WCCP or authentication.

Best-in-Class Cloud-Delivered Security Services Powered by Precision AI

The typical enterprise's attack surface has grown significantly with the mass adoption of hybrid work, cloud, IoT, and SaaS. Furthermore, the threat landscape is rapidly intensifying due to the ability to easily access and use hacker-friendly tools and resources in their campaigns. Traditional network security solutions and approaches are no longer effective. With Palo Alto Networks Cloud-Delivered Security Services, customers can benefit from best-in-class, real-time security to help them protect all users, devices, and data in their network, regardless of location.

Palo Alto Networks security services use the power of Precision AI® inline to stay ahead of threat actors and stop new and never-before-seen threats in real time. Through shared threat intelligence across over 70,000 customers worldwide, they have insights into emerging threats and can act proactively. Finally, seamless integration with NGFW and SASE eliminates security gaps and offers customers a single pane of glass to view and manage their security.

Services include:

- **Advanced Threat Prevention:** Stop known and unknown exploits, malware, spyware, and command-and-control (C2) threats, including 60% more injection attacks and 48% more highly evasive C2 traffic than traditional IPS solutions with industry-first zero-day attack prevention.
- **Advanced WildFire®:** Ensure safe access to files with the industry's largest malware prevention engine, stopping up to 22% more unknown malware and turning detection into prevention 180X faster than competitors.
- **Advanced URL Filtering:** Ensure safe access to the web and prevent 40% more threats in real time than traditional filtering databases with industry-first prevention of known and unknown phishing attacks, stopping up to 88% of malicious URLs at least 48 hours before competitors.
- **Advanced DNS Security:** Protect your DNS traffic and stop advanced DNS-layer threats, including DNS hijacking, all in real time with 2X more DNS-layer threat coverage than competitors.
- **Next-Generation CASB:** Discover and control all SaaS consumption in your network with visibility into 60K+ SaaS apps and protect your data with 28+ API integrations.
- **IoT Security:** Secure your blind spots and protect every connected device unique to your vertical with the industry's most comprehensive Zero Trust solution for IoT devices, discovering 90% of devices within 48 hours.

Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

Enables SD-WAN Functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end-user experience by minimizing latency, jitter, and packet loss.

Table 1: PA-3400 Series Performance and Capacities				
	PA-3410	PA-3420	PA-3430	PA-3440
Firewall throughput (appmix)*	14 Gbps	19 Gbps	29 Gbps	35 Gbps
Threat Prevention throughput (appmix)†	7.5 Gbps	10 Gbps	15 Gbps	20 Gbps
IPsec VPN throughput‡	6.6 Gbps	9.9 Gbps	12 Gbps	14.5 Gbps
Max concurrent sessions§	1.4M	2.2M	2.5M	3M
New sessions per second¶	145,000	220,000	240,000	268,000
Virtual systems (base/max)#	1/11	1/11	1/11	1/11

Note: Results were measured on PAN-OS 11.2.

* Firewall throughput is measured with App-ID and logging enabled, utilizing appmix transactions.

† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispysware, WildFire, file blocking, and logging enabled, utilizing appmix transactions.

‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.

§ Max concurrent sessions are measured utilizing HTTP transactions.

¶ New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.

Adding virtual systems over base quantity requires a separately purchased license.

Table 2: PA-3400 Series Networking Features	
Interface Modes	
L2, L3, tap, virtual wire (transparent mode)	
Routing	
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing	
Policy-based forwarding	
Point-to-Point Protocol over Ethernet (PPPoE)	
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3	
Bidirectional Forwarding Detection (BFD)	
IPsec and SSL VPN	
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)	
Encryption: 3des, AES (128-bit, 192-bit, 256-bit)	
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512	
GlobalProtect® large-scale VPN for simplified configuration and management*	
Secure access over IPsec and SSL VPN tunnels using GlobalProtect Gateway and portals*	
VLANs	
802.1Q VLAN tags per device/per interface: 4,094/4,094	
Aggregate interfaces (802.3ad), LACP	
Network Address Translation	
NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation)	
NAT64, NPTv6	
Additional NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription	

* Requires GlobalProtect license.

Table 2: PA-3400 Series Networking Features (continued)
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Mobile Network Infrastructure† (PA-3440 and PA-3430)
5G Security
GTP Security
SCTP Security

† For additional information, refer to our [ML-Powered NGFWs for 5G](#) datasheet.

Table 3: PA-3400 Series Hardware Specifications
I/O
PA-3410: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3420: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)
PA-3430: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
PA-3440: 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4), 40G/100G QSFP/QSFP28 (2)
Management I/O
100/1000 out-of-band management port (1)
100/1000 high availability (2), 10G SFP+ high availability (1)
RJ-45 console port (1), Micro USB (1)
Storage Capacity
480 GB SSD
Trusted Platform Module (TPM)
Integrated with TPM for secure boot, hardware root of trust, and securing system secrets.
Power Supply (Avg/Max Power Consumption)
Redundant 450-watt AC (133W/190W)
Max BTU/hr
650
Input Voltage Frequency
AC: 100–240 VAC (50–60Hz)
Max Current Consumption
AC: 1.9 A @ 100 VAC, 0.8 A @ 240 VAC
Mean Time Between Failure (MTBF)
22 years
Rack Mount Dimensions
1U, 19" standard rack 14.15" x 17.15" x 1.70"
Weight (Standalone Device/As Shipped)
15.5 lbs/25 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A

Table 3: PA-3400 Series Hardware Specifications (continued)

Certifications

See paloaltonetworks.com/company/certifications.html

Environment

Operating temperature: 32°F to 104°F, 0°C to 40°C

Nonoperating temperature: -4°F to 158°F, -20°C to 70°C

Humidity tolerance: 10% to 90%

Maximum altitude: 10,000 ft/3,048 m

Airflow: front to back



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.
strata_ds_pa-3400-series_031925



October 15, 2025

To Whom It May Concern:

On Behalf of the Global NextWave Partner Program team at Palo Alto Networks, this is to inform you the partnership between Palo Alto Networks, Inc. and:

SmartSec Technologies s.r.o.

Bratislava, Bratislava

Slovakia

At the time of this communication, **SmartSec Technologies s.r.o.** is classified as a Solution Provider at the **Registered** level partner respectively in the Palo Alto Networks NextWave Partner Program and is in good standing.

SmartSec Technologies s.r.o. is also currently set with the following Specializations : **none at this time.**

Thank you,

Michael Khoury
VP, Global Channel Programs
Palo Alto Networks



V Praze 14. října 2025

Potvrzení o partnerství se společností Palo Alto Networks

Potvrzujeme, že společnost SmartSec Technologies s.r.o., sídlem Jégeho 6, 821 08 Bratislava, IČO: 50 448 676 je autorizovaným a registrovaným obchodním partnerem společnosti Palo Alto Networks pro Slovensko.

Za společnost Palo Alto Networks

Tom Horák
Channel Business Manager CZ/SK/HU/UA



BUREAU
VERITAS

Bureau Veritas Certification

Certifikát

udelený organizácii

Aricoma Systems s.r.o.

Krasovského 14, 851 01 Bratislava-mestská časť Petržalka, Slovenská republika

BUREAU VERITAS CERTIFICATION CZ, s.r.o. týmto potvrdzuje, že systém manažérstva vyššie uvedenej organizácie bol preverený a bolo preukázané, že tento systém spĺňa požiadavky nižšie uvedenej normy:

Norma

ČSN EN ISO 9001:2016

Oblasť certifikácie

NÁKUP A PREDAJ TOVARU A IT SLUŽIEB.
POSKYTOVANIE SERVISNÝCH SLUŽIEB IT.
RIADENIE PROJEKTOV.
HELPDESK.
VZDIALENÁ SPRÁVA A DOHL'AD.
NÁVRH A VÝVOJ SOFTVÉRU.

Dátum počiatočného schválenia

06-09-2021

Počiatočný dátum certifikačného/ recertifikačného cyklu:

01-07-2024

Konečný dátum certifikačného/ recertifikačného cyklu:

30-06-2027

Za predpokladu udržiavania účinného systému manažérstva v organizácii tento certifikát platí do:

30-06-2027

Pre overenie platnosti certifikátu môžete kontaktovať: +420 210 088 215

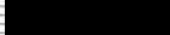
Ďalšie objasnenie ohľadne predmetu tohto certifikátu a aplikovateľnosti požiadaviek na uvedený systém môžete získať kontaktovaním organizácie.



Verzia 2

Dátum vydania: 01-07-2024

Číslo certifikátu:



MANAGING OFFICE: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic

ISSUING OFFICE ADDRESS: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic



BUREAU
VERITAS

Bureau Veritas Certification

Certifikát

udelený organizácii

Aricoma Systems s.r.o.

Krasovského 14, 851 01 Bratislava-mestská časť Petržalka, Slovenská republika

BUREAU VERITAS CERTIFICATION CZ, s.r.o. týmto potvrdzuje, že systém manažmentu služieb v informačných technológiách vyššie uvedenej organizácie bol preverený a bolo preukázané, že tento systém spĺňa požiadavky nižšie uvedenej systémovej normy:

Norma

ČSN ISO/IEC 20000-1:2019

Oblasť certifikácie

POSKYTOVANIE KOMPLEXNÝCH ICT SLUŽIEB

Dátum počiatočného schválenia **02-04-2023**

Počiatočný dátum certifikačného/ recertifikačného cyklu: **01-07-2024**

Konečný dátum certifikačného/ recertifikačného cyklu: **30-06-2027**

Za predpokladu udržiavania účinného systému manažérstva v organizácii tento certifikát platí do: **30-06-2027**

Pre overenie platnosti certifikátu môžete kontaktovať: +420 210 088 215

Ďalšie objasnenie ohľadne predmetu tohto certifikátu a aplikovateľnosti požiadaviek na uvedený systém môžete získať kontaktovaním organizácie.



Verzia 2 Dátum vydania: 01-07-2024

Číslo certifikátu:



MANAGING OFFICE: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic

ISSUING OFFICE ADDRESS: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic



BUREAU
VERITAS

Bureau Veritas Certification

Certifikát

udelený organizácii

Aricoma Systems s.r.o.

Krasovského 14, 851 01 Bratislava, Slovenská republika

BUREAU VERITAS CERTIFICATION CZ, s.r.o. týmto potvrdzuje, že systém manažérstva bezpečnosti informácií vyššie uvedenej organizácie bol preverený a bolo preukázané, že tento systém spĺňa požiadavky nižšie uvedenej systémovej normy:

Norma

ČSN EN ISO/IEC 27001:2023

Oblasť certifikácie

DODÁVKA A PREVÁDZKA IT INFRAŠTRÚKTURY PRE ZÁKAZNÍKOV.

v rozsahu pôsobnosti vyhlásenia o aplikovateľnosti verzia 3 zo 17.9.2024

Dátum počiatočného schválenia 02-04-2023

Počiatočný dátum certifikačného/ recertifikačného cyklu 18-10-2024

Konečný dátum certifikačného/ recertifikačného cyklu 17-10-2027

Za predpokladu udržiavania účinného systému manažérstva v organizácii tento certifikát platí do 17-10-2027

Pre overenie platnosti certifikátu môžete kontaktovať: +420 210 088 215

Ďalšie objasnenie ohľadne predmetu tohto certifikátu a aplikovateľnosti požiadaviek na uvedený systém môžete získať kontaktovaním organizácie.



Verzia 1 Dátum vydania: 18-10-2024

Číslo certifikátu:



MANAGING OFFICE: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic

ISSUING OFFICE ADDRESS: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic



BUREAU
VERITAS

Bureau Veritas Certification

Certifikát

udelený organizácii

Aricoma Systems s.r.o.

Krasovského 14, 851 01 Bratislava-mestská časť Petržalka, Slovenská republika

BUREAU VERITAS CERTIFICATION CZ, s.r.o. týmto potvrdzuje, že systém manažérstva vyššie uvedenej organizácie bol preverený a bolo preukázané, že tento systém spĺňa požiadavky nižšie uvedenej normy:

Norma

ČSN EN ISO 14001:2016

Oblasť certifikácie

NÁKUP A PREDAJ TOVARU A IT SLUŽIEB.
POSKYTOVANIE SERVISNÝCH SLUŽIEB IT.
RIADENIE PROJEKTOV.
HELPDESK.
VZDIALENÁ SPRÁVA A DOHLAD.
NÁVRH A VÝVOJ SOFTVÉRU.

Dátum počiatočného schválenia

06-09-2021

Počiatočný dátum certifikačného/ recertifikačného cyklu:

01-07-2024

Konečný dátum certifikačného/ recertifikačného cyklu:

30-06-2027

Za predpokladu udržiavania účinného systému manažérstva v organizácii tento certifikát platí do:

30-06-2027

Pre overenie platnosti certifikátu môžete kontaktovať: +420 210 088 215

Ďalšie objasnenie ohľadne predmetu tohto certifikátu a aplikovateľnosti požiadaviek na uvedený systém môžete získať kontaktom s organizáciou.



Verzia 2

Dátum vydania: 01-07-2024

Číslo certifikátu:



MANAGING OFFICE: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic

ISSUING OFFICE ADDRESS: BUREAU VERITAS CERTIFICATION CZ, s.r.o., Olbrachtova 1, 140 02 Praha 4, Czech Republic

Čestné vyhlásenie

Spoločnosť **SmartSec Technologies s.r.o.** týmto prehlasuje, že disponuje vlastným systémom nahlasovania väd v režime 24/7.

Tecnnická podpora

Technickú podporu pre klientov zabezpečujeme aj prostredníctvom mobilnej alebo mailovej komunikácie.

Kontakty:

Mail: support@smartsectechnologies.sk

Mobil:

S úctou

Jozef Dobiš

konateľ