904 093 778

Kupní smlouva

č. j.: NA-4862-29/01-2025

podle ust. § 2079 a násl. občanského zákoníku, v platném znění

(dále jen „smlouva")

Česká republika – Národní archiv
se sídlem Archivní 2257/4, 149 00 Praha 4 – Chodov
IČO: 70979821
zastoupena: PhDr. Ing. Milanem Vojáčkem, Ph.D., ředitelem Národního archivu
Bankovní spojení:
Číslo účtu:
Kontaktní osoba:
Tel. / email:
Kontaktní osoba:
Tel. / email:
ID datové schránky: fe3aixh
(dále jen „**Kupující**")

a

CompuNet s. r. o.
Zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 118594
se sídlem Zubatého 295/5, 150 00 Praha 5
IČ: 27608514
DIČ: CZ27608514
zastoupena: Ing. Pavlem Pikhartem, jednatelem
Bankovní spojení:
Číslo účtu:
Kontaktní osoba:
Tel. / email:
ID datové schránky: kw6wenn
(dále jen „**Prodávající**")

(dále také Kupující a Prodávající společně označovaní jako „Smluvní strany" nebo jednotlivě „Smluvní strana")

se společně dohodli na kupní smlouvě následujícího znění:

1. ÚČEL A PŘEDMĚT SMLOUVY

1.1. Tato smlouva je uzavírána mezi Kupujícím a Prodávajícím na základě výsledků výběrového řízení za účelem realizace veřejné zakázky malého rozsahu s názvem **„Nákup VPN koncentrátoru včetně poskytování technické podpory**", systémové číslo veřejné zakázky na profilu Kupujícího jakožto zadavatele, NEN: **N006/25/V00030594 (dále jen „veřejná zakázka"), zadávané v souladu s ust. § 31 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále také jen jako „ZZVZ"), mimo jeho působnost formou otevřené výzvy. Nabídka Prodávajícího podaná v rámci výběrového řízení na Veřejnou zakázku byla vyhodnocena jako ekonomicky nejvýhodnější.**

Předmětem této smlouvy je povinnost Prodávajícího dodat a implementovat Kupujícímu **VPN cluster** sestavený ze dvou identických Next Generation firewallů (NGFW) v režimu vysoké dostupnosti (HA), respektující stávající segmentaci sítě, specifičnost a režimy, které jsou aktuálně realizovány a využívány, kdy součástí plnění rovněž musí být pokrytí veškerými potřebnými licencemi, licencemi pro služby zajišťujícími bezpečnost (AM/AV, DPI, IDS/IPS, aplikační kontrola, filtrace URL atd.), zárukami a podporou (dále jen „zboží"), který je blíže specifikován v **Příloze č. 1a – „Předmět zakázky" a Příloze č. 1b – „Podrobná specifikace zakázky"** smlouvy a to řádně, včas a za podmínek upravených v zadávacích podmínkách na Veřejnou zakázku, v nabídce podané Prodávajícím v rámci zadávacího řízení na Veřejnou zakázku a za podmínek uvedených dále v této smlouvě a jejích přílohách.

1.2. Předmětem této smlouvy je dále závazek Kupujícího řádně a včas dodané zboží převzít a zaplatit za ně Prodávajícímu cenu za podmínek stanovených v článku 3 této smlouvy.

2. TERMÍN DODÁNÍ A MÍSTO PLNĚNÍ

2.1. Prodávající se zavazuje dodat zboží Kupujícímu **do 8 týdnů** po nabytí platnosti a účinnosti této smlouvy, **nejpozději však do 15. 12. 2025**. Předpoklad uzavření smlouvy je nejpozději do 14. 10. 2025. Řádné převzetí zboží potvrdí oprávněný zástupce Kupujícího podpisem na dodacím listu.

2.2. Místem plnění je sídlo Kupujícího, uvedené výše v této smlouvě, nebude-li mezi Smluvními stranami dohodnuto písemně jinak. Kontaktní osobou je [redacted] Prodávající není oprávněn měnit místo plnění bez předchozího písemného souhlasu Kupujícího.

3. CENOVÉ A PLATEBNÍ PODMÍNKY

3.1. Kupní cena za dodání zboží (dále jen „ kupní cena") je stanovena na základě nabídkové ceny Prodávajícího, která byla předložena v rámci výběrového řízení.

3.2. Kupní cena dle odst. 3. 1. činí:

Název položky	Požadovaný počet měrných jednotek	Cena za jednu měrnou jednotku položky bez DPH	Cena celkem za položku bez DPH	Celkem DPH za položku	Cena celkem za položku s DPH
VPN koncentrátor	1 ks	503 218,00	503 218,00	105 675,78	608 893,78
Zajištění následné technické a kyberbezpečnostní podpory ze strany Poskytovatele v průběhu následujících 60 ti měsíců ve formě opce na 75 h práce Poskytovale na vyžádání Zadavatelem	75 h	2 000,00	150 000,00	31 500,00	181 500,00
Ceny celkem	X	X	653 218,00	137 175,78	790 393,78

Cena celkem za zakázku s DPH slovy:
Sedm set devadesát tisíc tři sta devadesát tři korun českých sedmdesát osm haléřů

3.3. Kupní cena je stanovena dohodou Smluvních stran jako cena nejvýše přípustná, nepřekročitelná po dobu realizace této smlouvy a jsou v ní zahrnuty veškeré náklady prodávajícího spojené s dodáním zboží.

3.4. Kupní cenu je možné překročit pouze v souvislosti se změnou daňových předpisů upravujících výši DPH, přičemž v takovém případě bude k ceně připočteno DPH ve výši stanovené platným a účinným zákonem č. 235/2004 Sb., o dani z přidané hodnoty.

3.5. Kupní cena bude Prodávajícím uhrazena v korunách českých (CZK) na základě jediného řádného daňového dokladu (dále jen „faktura") doručeného Kupujícímu.

3.6. Faktura, musí obsahovat všechny náležitosti řádného daňového dokladu ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Nedílnou součástí faktury budou všechny dodací listy. V případě, že faktura bude obsahovat věcné či formální nesprávnosti, popřípadě nebude obsahovat všechny zákonné náležitosti nebo přílohy, je Kupující oprávněn ji vrátit ve lhůtě splatnosti zpět Prodávajícímu k doplnění či opravě, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury Kupujícímu.

3.7. Splatnost faktury se sjednává na **30 dnů** ode dne doručení faktury Kupujícímu.

3.8. Faktura bude zaslána v elektronickém vyhotovení do datové schránky Kupujícího: fe3aixh, nebo na e-mailovou adresu: [redacted] se specifikací, že adresátem je Oddělení

digitalizace a digitálního archivu Národního archivu.

3.9. Kupující je oprávněn vrátit fakturu do konce doby její splatnosti zpět Prodávajícímu, pokud bude obsahovat nesprávné nebo neúplné náležitosti či údaje anebo pokud požadované náležitosti a údaje nebude obsahovat vůbec. V takovém případě nová doba splatnosti počíná běžet ode dne doručení opravené nebo doplněné faktury Kupujícímu. Kupující není v takovém případě v prodlení.

3.10. Prodávající není oprávněn, bez předchozího písemného souhlasu Kupujícího, provádět jakékoliv zápočty svých pohledávek vůči Kupujícímu proti jakýmkoliv pohledávkám Kupujícího vůči Prodávajícímu. Prodávající není oprávněn postoupit pohledávku nebo její část vůči Kupujícímu na třetí osoby.

3.11. Kupující neposkytuje Prodávajícímu zálohy na cenu.

3.12. Fakturace za poskytování technické podpory po dobu 60 měsíců, pokud bude objednatelem využita, bude prováděna zvlášť, a to vždy po schválení čerpání hodin prací, oběma smluvními stranami za daný kalendářní měsíc.

3.13. Objednatel je organizační složkou státu a tedy neplátcem DPH ve smyslu zákona č. 234/2005 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Z tohoto důvodu na objednatele nemůže být přenesena daňová povinnost podle cit. zákona.

4. PŘEDÁNÍ A PŘEVZETÍ LICENCÍ, PŘECHOD VLASTNICTVÍ

4.1. Vlastnické právo ke zboží podle této smlouvy přechází z Prodávajícího na Kupujícího okamžikem jeho převzetí.

4.2. Nebezpečí škody na věci přechází na Kupujícího okamžikem převzetí zboží.

4.3. Budou-li při předání zboží zjištěny vady zboží (za vadu se považuje i plnění jiné věci, jakož i vady v dokladech vztahujících se ke zboží), bude po konkrétním vymezení zjištěných vad stanoven způsob a termín jejich odstranění. Zboží se považuje za řádně předané až po odstranění všech vad. Kupující je oprávněn zboží nepřevzít, má-li pro to vážný důvod.

5. PRÁVA Z VAD, SANKCE, ODSTOUPENÍ OD SMLOUVY

5.1. Prodávající se zavazuje poskytnout Kupujícímu na zboží záruku za jakost, garantovanou výrobcem, **v délce 60 měsíců**, a to počínaje dnem převzetí zboží Kupujícím dle čl. 4. této smlouvy.

5.2. Vady musí Kupující uplatnit u Prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

5.3. Vyskytne-li se vada v záruční době a neuplatní-li Kupující jiný nárok z vadného plnění, je Prodávající povinen nastoupit k odstranění vady následující pracovní den po oznámení vady Kupujícímu, a to v místě instalace či umístění zboží, a vadu bezplatně odstranit v termínu dohodnutém s Kupujícím, nejpozději však do 30 kalendářních dnů od doručení písemného oznámení vady Kupujícím. O odstranění vady bude pořízen protokol podepsaný oběma Smluvními stranami.

5.4. Kupující má právo na úhradu nutných nákladů, které mu vznikly v souvislosti s uplatněním práv z vadného plnění.

5.5. Za záruční vady nebudou považovány ty vady, které byly způsobeny nesprávnou či neodbornou manipulací Kupujícího se zbožím, obsluhou, údržbou nebo úmyslným

poškozením zboží Kupujícím nebo nepovolanou osobou, případně jakýmikoli jinými zásahy, jednáními nebo skutečnostmi nastalými na straně Kupujícího. Odstranění takto zjištěných vad bude provedeno za úplatu.

5.6. Je-li vadné plnění podstatným porušením této smlouvy, má Kupující právo na odstranění vady dodáním nového zboží bez vady nebo dodáním chybějícího zboží, na odstranění vady opravou zboží, na přiměřenou slevu nebo odstoupení od této smlouvy. Smluvní strany se dohodly, že za podstatné porušení smlouvy bude považováno zejména:

a) nemožnost odstranění vady dodaného zboží, a to ani výměnou za nové zařízení;
b) prodlení Prodávajícího s dodáním zboží dle čl. 2. odst. 2.1. této smlouvy o více než 7 kalendářních dnů;
c) prodlení Prodávajícího s odstraněním vady v záruční době dle odst. 5.3. tohoto článku o více než 14 kalendářních dní;
d) jestliže Prodávající ujistil Kupujícího, že zboží má určité vlastnosti, zejména vlastnosti Kupujícím výslovně vymíněné, anebo že nemá žádné vady, a toto ujištění se následně ukáže nepravdivým.

5.7. Kupující je dále oprávněn odstoupit od smlouvy, jestliže zjistí, že Prodávající:

a) nabízel, dával, přijímal nebo zprostředkovával určité hodnoty s cílem ovlivnit chování nebo jednání kohokoliv, ať již státního úředníka nebo někoho jiného, přímo nebo nepřímo, v zadávacím řízení nebo při provádění smlouvy; nebo
b) zkresloval jakékoliv skutečnosti za účelem ovlivnění zadávacího řízení nebo provádění smlouvy ke škodě Kupujícího, včetně užití podvodných praktik k potlačení a snížení výhod volné a otevřené soutěže; nebo
c) nedodržoval povinnosti vyplývající z předpisů práva životního prostředí, sociálních nebo pracovně právních předpisů nebo kolektivních smluv vztahujících se k předmětu plnění Veřejné zakázky.

5.8. Prodávající může od této smlouvy odstoupit, pokud:

a) je Kupující v prodlení s úhradou faktury Prodávajícího za dodané zboží déle než 60 kalendářních dnů ode dne jejího doručení Kupujícímu, a zároveň
b) byl Kupující na její neuhrazení písemně Prodávajícím upozorněn spolu s možným důsledkem odstoupení od této smlouvy, a po tomto upozornění ji Kupující do 7 kalendářních dní neuhradil.

5.9. Smluvní strany mohou tuto smlouvu ukončit dohodou nebo odstoupením, vždy v písemné formě. Odstoupením se závazek založený smlouvou zrušuje od počátku a Smluvní strany se vypořádají podle příslušných ustanovení Občanského zákoníku o bezdůvodném obohacení. Účinky odstoupení od smlouvy nastávají okamžikem doručení písemného oznámení o odstoupení od smlouvy Prodávajícímu. Odstoupení od smlouvy se nedotýká práva na zaplacení smluvní pokuty a úroku z prodlení, pokud již dospěl, práva na náhradu škody ani ujednání, které má vzhledem ke své povaze zavazovat Smluvní strany i po odstoupení od smlouvy, tj. zejména nikoli však výlučně ani ujednání o způsobu řešení sporů a volbě práva. Obdobné platí i pro předčasné ukončení smlouvy jiným způsobem.

5.10. Bude-li Kupující v prodlení s úhradou faktury, je Prodávající oprávněn požadovat úhradu úroku z prodlení z dlužné částky ve výši stanovené příslušnými právními předpisy.

5.11. Při nedodržení doby dodání zboží či v případě prodlení s odstraněním vady zboží je Prodávající povinen uhradit Kupujícímu smluvní pokutu ve výši 0,05 % z ceny za každý i započatý den prodlení.

5.12. Smluvní pokuta je splatná do 30 kalendářních dnů ode dne doručení výzvy k jejímu zaplacení Prodávajícímu. Dnem splatnosti se rozumí den připsání příslušné částky na účet Kupujícího.

5.13. Uplatněním práv z vad či uplatněním smluvních pokut není dotčeno právo na náhradu škody (újmy) v její plné výši.

6. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

6.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění závazků vyplývajících z čl. 1. této smlouvy.

6.2. Veškerá komunikace bude probíhat prostřednictvím oprávněných osob Smluvních stran. Oprávněné osoby budou zastupovat Smluvní strany ve smluvních a obchodních záležitostech souvisejících s plněním této smlouvy. Pro účely této smlouvy se má za to, že oprávněnými osobami jsou kontaktní osoby uvedené výše.

6.3. Změna oprávněné osoby je možná jen po předchozím písemném oznámení této skutečnosti druhé Smluvní straně, avšak nevyžaduje uzavření dodatku k této smlouvě.

7. ZÁVĚREČNÁ USTANOVENÍ

7.1. Prodávající se zavazuje zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od Kupujícího v souvislosti s plněním předmětu této Smlouvy. Tato povinnost mlčenlivosti se vztahuje na všechny zaměstnance a spolupracovníky Prodávajícího. Povinnost mlčenlivosti přetrvá i po ukončení této smlouvy.

7.2. Prodávající prohlašuje, že není předlužen a není mu známo, že by bylo vůči němu zahájeno insolvenční řízení. Dále prohlašuje, že vůči němu není vydáno žádné soudní rozhodnutí, či rozhodnutí správního, daňového či jiného orgánu nebo rozhodce na plnění, které by mohlo být důvodem soudní exekuce na majetek Prodávajícího, nebo by mohlo mít, jakkoliv negativní vliv na schopnost Prodávajícího splnit povinnosti vyplývající z této smlouvy, a že takové řízení nebylo vůči němu zahájeno a že ani nehrozí zahájení takového řízení.

7.3. Tato smlouva a práva a povinnosti z ní vyplývající se řídí právním řádem České republiky. Práva a povinnosti Smluvních stran, pokud nejsou upraveny touto smlouvou, se řídí Občanským zákoníkem a předpisy souvisejícími. Rozhodčí řízení je vyloučeno.

7.4. Veškeré případné spory vzniklé mezi Smluvními stranami na základě nebo v souvislosti s touto smlouvou budou primárně řešeny jednáním Smluvních stran. V případě, že tyto spory nebudou v přiměřené době vyřešeny, budou k jejich projednání a rozhodnutí příslušné obecné soudy České republiky.

7.5. Prodávající se zavazuje k součinnosti při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů. Prodávající se dále zavazuje umožnit všem oprávněným subjektům provést kontrolu dokladů souvisejících s plněním Veřejné zakázky, a to po dobu určenou k jejich archivaci v souladu s příslušnými právními předpisy.

7.6. Prodávající podpisem této smlouvy bere na vědomí, že Kupující je ve smyslu nařízení č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR), správcem osobních údajů subjektu údajů, a že tyto osobní údaje sám zpracovává a shromažďuje pro účely realizace této smlouvy, bez využití zpracovatele údajů.

7.7. Prodávající souhlasí s tím, aby Kupující po dobu trvání této smlouvy zpracovával jeho osobní údaje uvedené v této smlouvě a údaje o této smlouvě pro účely archivace, či případné kontrolní činnosti nebo pro účely vyplývající z právních předpisů. Dále svým podpisem uděluje souhlas Kupujícímu ke zpracování jeho osobních údajů ve výše uvedeném rozsahu a pro výše uvedené účely, a to po dobu nezbytně nutnou.

7.8. Prodávající bezvýhradně souhlasí se zveřejněním své identifikace a dalších parametrů smlouvy včetně ceny v souladu s příslušnými právními předpisy.

7.9. Tato smlouva může být měněna nebo doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oběma Smluvními stranami. Ke změnám či doplnění neprovedeným písemnou formou se nepřihlíží.

7.10. V případě, že některé ustanovení této smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým shledáno příslušným orgánem, zůstávají ostatní ustanovení této smlouvy v platnosti a účinnosti, pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž byla tato smlouva uzavřena, nevyplývá, že jej nelze oddělit od ostatního obsahu této smlouvy. Smluvní strany se zavazují bezodkladně nahradit neplatné, neúčinné nebo nevymahatelné ustanovení této smlouvy ustanovením jiným, které svým obsahem a smyslem odpovídá nejlépe ustanovení původnímu a této smlouvě jako celku.

7.11. Smluvní strany na sebe přebírají nebezpečí změny okolností v souvislosti s právy a povinnostmi Smluvních stran vzniklými na základě této smlouvy. Smluvní strany vylučují uplatnění ustanovení § 1765 odst. 1 a § 1766 Občanského zákoníku na svůj smluvní vztah založený touto Smlouvou.

7.12. Tato smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v Informačním systému Registr smluv (dále jen „**IS RS**") dle podmínek stanovených zejména zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění této Smlouvy v IS RS provede Kupující.

7.13. Tato smlouva je uzavřena v listinné nebo elektronické podobě. Je-li smlouva uzavřena v listinné podobě, je podepsána vlastnoručně Smluvními stranami a vyhotovena

ve 3 stejnopisech, z nichž každý bude považován za prvopis, přičemž 2 stejnopisy smlouvy obdrží Kupující a 1 stejnopis obdrží Prodávající. Je-li Smlouva uzavřena v elektronické podobě, pak je její jediný elektronický originál podepsán pomocí uznávaných elektronických podpisů osob oprávněných jednat za Smluvní strany.

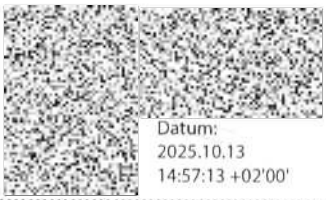
7.14. Zhotovitel je povinen archivovat veškerou dokumentaci a účetní doklady, související s realizací díla po dobu 10-ti let od ukončení a umožnit přístup k těmto dokladům.

7.15. Nedílnou součástí této smlouvy jsou následující přílohy:
Příloha č. 1a – „Předmět zakázky" a 1b – „Podrobná specifikace zakázky"

Smluvní strany prohlašují, že tato Smlouva vyjadřuje jejich svobodnou, vážnou, určitou a srozumitelnou vůli prostou omylu. Smluvní strany si Smlouvu přečetly, s jejím obsahem souhlasí, což stvrzují vlastnoručními podpisy.

V Praze

za Kupujícího:

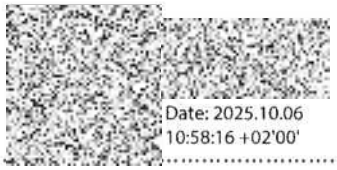


.....

PhDr. Ing. Milan Vojáček, Ph.D.
ředitel Národního archivu

V Praze

za Prodávajícího:



.....

Ing. Pavel Pikhart
jednatel

Předmět zakázky: *VPN koncentrátor*

Zadavatel požaduje řešení, které umožní zabezpečený přístup do jeho vnitřních sítí (segmentů, včetně DMZ) ze sítí veřejných pomocí technologie VPN (Virtual Private Network) a to jak pro interní uživatele (zaměstnance), tak pro spolupracující externí osoby, či zástupce dodavatelů. Předpokládaný počet VPN klientů je 200, současně připojených 50.

Zadavatel prohlašuje, že je provozovatelem VIS dle zákona č. 181/2014 Sb. ve znění vyhlášky 82/2018 Sb. a je povinen řídit se Zásadami KyBez resortu MV a jako osoba povinná i nařízeními, opatřeními a doporučeními NÚKIB.

Předmětem plnění je dodávka a implementace VPN clusteru sestaveného ze dvou identických Next Generation firewallů (NGFW) v režimu vysoké dostupnosti (HA), respektující stávající segmentaci sítě, specifičnost a režimy, které jsou aktuálně realizovány a využívány, kdy součástí plnění rovněž musí být pokrytí veškerými potřebnými licencemi, licencemi pro služby zajišťujícími bezpečnost (AM/AV, DPI, IDS/IPS, aplikační kontrola, filtrace URL atd.), zárukami a podporou v požadovaném rozsahu, to vše po dobu nejméně 5 let (60 měsíců). Výsledný cluster dvou VPN koncentrátorů bude zajišťovat zabezpečené připojení pracovníků Zadavatele a jím pověřených osob v rámci standartu SSL VPN.

Zadavatel předpokládá využití hlavní a záložní konektivity do veřejných sítí o rychlosti nejméně 1Gbps (v daném okamžiku Zadavatel disponuje konektivitou realizovanou prostřednictvím bezdrátové technologie s garantovanou symetrickou propustností 100Mbps, zakončenou v datovém centru Zadavatele; Zadavatel očekává rozšíření konektivity v průběhu roku 2026 prostřednictvím technologií optických sítí), dále připojení do CMS2 prostřednictvím 3 dedikovaných linek o kapacitách 500 a 2x100 Mbps. Všechny konektory na straně Zadavatele jsou (budou) realizovány metalickými RJ-45.

Zadavatel provozuje AD na platformě MS Windows server 2016 - jedná se o doménovou síť - interní uživatel má svůj účet v doméně nacr.cz. Pro vlastní sestavení VPN bude u interních uživatelů akceptována 2FA, založená na proprietárním resortním řešení. Toto je realizováno čipovou kartou STARCOS s čipem 3.7 C3, kdy je v jejím zabezpečeném úložišti uložen přístupový (komerční) certifikát vydaný NCA. Karta je ke klientskému systému připojena USB čtečkou (výrobce ACS) prostřednictvím middleware s názvem SecureStore (aktuálně ve verzi 8.0.1). **Pro Zadavatele je tento požadavek na podporovanou a funkční 2FA naprosto zásadní a vyhrazuje si před převzetím předmětu plnění plně otestovat funkčnost řešení!** SLL VPN koncentrátor však zároveň bude zajišťovat i připojení pro externí pracovníky do jiných segmentů sítě; proto tyto pracovníky se nebude využívat ověření přes čipové karty s čipem Starcos 3.7. C3, avšak může být vynucováno dodržení jiných pravidel, např. přístup z konkrétní IP (zdrojová IP či adresní rozsah), časové „okno", či aktivní spolupráce (on demand) třetí osoby s osobou pověřenou Zadavatelem (např. interní správce/administrátor) k takovému postupu.

Zadavatel požaduje, aby Poskytovatel provedl analýzu prostředí Zadavatele pro implementaci v rozsahu, který Poskytovatel požaduje za přiměřený, dále představil a detailně popsal návrh řešení v nabídce (s důrazem na vyřešení 2FA); součástí vlastní dodávky pak bude dokumentace atd. (viz. část „Nedílná součást dodávky" v závěru tohoto dokumentu); cena této součásti plnění musí být Poskytovatelem stanovena jako konečná a nepřekročitelná a musí být součástí ceny celého dodávaného řešení.

Zadavatel požaduje dodání „na klíč", tedy včetně funkční a otestované konfigurace, založené na analýze prostředí, požadavků a zvyklostí Zadavatele Poskytovatelem. Zadavatel požaduje předání plně produkčního řešení v určených lokalitách (Archivní 4 a Archivní 6) a to včetně zajištění případné následné budoucí technické a kyberbezpečnostní podpory (např. ad-hoc fixace objevených zranitelností, související aktualizace firmware, IDS/IPS, AV, aplikační kontroly, filtrace URL, atd., změny konfigurace, segmentace a další změny požadované Zadavatelem) ze strany Poskytovatele v průběhu následujících 60 měsíců ve formě opce na celkem 75 hodin práce Poskytovatele „na vyžádání" Zadavatelem, kdy Zadavatel požaduje, aby součástí návrhu řešení byla uvedena výše fixní hodinové sazby Poskytovatele platná pro výše uvedené období 60 měsíců. **Poskytovatel po dodání NEBUDE standardně disponovat přímým přístupem k dodanému řešení a veškeré budoucí zásahy tak bude možné provádět pouze pod dohledem Zadavatele při fyzické přítomnosti zástupce Poskytovatele v určených lokalitách Zadavatele; nepředvídatelné okolnosti však mohou být důvodem k přijetí dočasné výjimky z tohoto požadavku.**

Zadavatel požaduje, aby požadovaná zařízení (firewally) byla realizována ve formátu HW appliance v provedení pro instalaci do 19" racku. Zařízení následně budou instalována v klimatizovaném a zálohovaném (UPS) DC Zadavatele. Všechna připojení budou realizována metalickými RJ-45 konektory.

Zadavatel požaduje, aby řešení umožňovalo sestavení VPN pro uživatele, jejichž klientskými operačními systémy jsou MS Windows, iOS, macOS, Android, Linux v edicích Debian a Fedora.

Zadavatel požaduje bezvýpadkové plnění, tedy nasazení technologií způsobem, který neohrozí služby Zadavatelem poskytované, ani běžné plnění úkolů.

Zadavatel rovněž požaduje komunikaci pracovníků Poskytovatele v českém jazyce, reakční dobu na požadavek/opatření/doporučení typu KB událost 48h, požadavek/opatření/doporučení typu KB incident 24h; řešení provozních nedostatků při kolapsu HA nejpozději NBD. Zadavatel požaduje připojení na dohledové centrum eGovernmentu pomocí Syslog.

Zadavatel požaduje předání řešení Poskytovatelem včetně zaškolení pracovníků Zadavatele pro správu, uživatelskou obsluhu, monitoring a vyhodnocování provozních stavů zařízení. Správci pověření Zadavatelem z řad jeho zaměstnanců musí být schopni provádět aktualizace zařízení, jejich konfiguraci a rovněž údržbu.

Zadavatel předpokládá připojení SIEM či jiných nástrojů pro real-on-time analýzu logů a výstupu analytických nástrojů koncentrátorů. Požadováno je zasílání logů pomocí syslogu.

Technická specifikace: *viz. Příloha s názvem „VPN koncentrátor – specifikace.xlsx"*

Nedílnou součástí dodávky (instalačních a implementačních prací) musí být:

- Analýza prostředí Zadavatele, konfigurací stávajících zařízení, topologie sítí a její segmentace;
- návrh nového uspořádání s důrazem na bezpečnost, odolnost a efektivitu při naplňování požadavků a úkolů, které je Zadavatel povinen řešit v souvislosti s ISMS rezortu MV, KyBez a doporučení NÚKIB;
- montáž a instalace dodaných zařízení do 19" serverových rozvaděčů v součinnosti se Zadavatelem; bezvýpadkové nasazení;
- konfigurace a připojení všech dodaných zařízení do síťové infrastruktury Zadavatele;
- aktualizace firmware a SW v dodaných zařízeních na poslední doporučené verze;
- integrace VPN koncentrátorů s ostatními technologiemi Zadavatele – segmenty sítě (včetně DMZ), MS Active Directory (test členství v příslušné bezpečnostní skupině), NTP a další...; otestování před nasazením do ostrého provozu;
- konfigurace, nastavení a spuštění VPN koncentrátoru a bezpečnostních funkcí pro ochranu uživatelů připojujících se přes VPN;
- součinnost se Zadavatelem v rámci instalace VPN klientů na koncové stanice, vlastní instalaci na koncové stanice bude Zadavatel provádět vlastními silami;
- zaškolení pracovníků Zadavatele a vytvoření dokumentace (provozní, bezpečnostní, uživatelské);
- vypracování DRP pro scénáře případů výpadku napájení, konektivity, apod.; otestování.

Příloha č. 1b – Podrobná specifikace zakázky

VPN koncentrátor s podporou 2FA

	Splňuje ANO/NE	Popis splnění
Základní požadavky:		
Bezpečnostní zařízení typu next-generation firewall (dále též pouze NGFW) musí být jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic apod. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW	ANO	Nabízené zařízení Palo Alto Networks PA-440 je řízení typu next-generation firewall a je jako jeden celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic a pod. Podpora výrobcem PaloAlto je zajištěna po dobu plánované životnosti NGFW
Výrobce NGFW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls v posledním aktuálním reportu společnosti Gartner	ANO	Výrobce PaloAlto je uveden jako Leaders v kvadrantu Entreprise Network Firewalls společnosti Gartner
Zařízení a/nebo jeho operační stystém, systém centrální sprvávy musí být certfikován dle FIPS 140-3	ANO	Firewall (VPN koncentrátor) je certifikován dle FIPS 140-3
Požadavky na HW architekturu:		
Musí být dostupný jako HW appliance, virtuální appliance nebude akceptována	ANO	Nabízený VPN koncentrátor - firewall bude dodán jako HW apliance. Nebude dodán jako virtuální apliance.
Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"	ANO	V nabídce jsou uvedeny parametry požadavané zadavatelem jsou uváděny tj. v real world mix paketech, tzv. "application mix"
Modul pro zpracování dat musí být v architektuře firewallu oddělen alespoň na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění	ANO	Architektura firewallu je oddělená tj. modul pro zpracování dat je v architektuře firewallu oddělen na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti) a nedochází k jejich vzájemnému ovlivnění

Musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	Obsahuje 1x dedikovaný management port pro přístup k CLI
Musí obsahovat minimálně 8 metalických datových rozhraní o rychlosti 1Gb/s	ANO	Obsahuje 8 x 1GbE metalické Ethernet porty
Musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu NGFW	ANO	Obsahuje 1x dedikovaný OOB management port pro plnohodnotnou správu NGFW
Musí být schopen ukládat logové údaje na interní storage o velikosti minimálně 120 GB	ANO	Obsahuje 128 GB eMMC storage pro logy
Musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	Plná podpora LACP 802.ad
Musí být rozměrově kompatibilní s 19" rozvaděčem	ANO	Zařízení je kompatibilní s rozvadečem o velikosti 19"
Musí podporovat dva nezávislé redundantní zdroje napájení AC 230V	ANO	Podporuje 2x nezávislé reduntantní zdroje napájení AC 230V

Požadavky na High Availability (HA):		
Požadujeme režim HA v módu Active-Active složený alespoň ze dvou zařízení	ANO	Součástí jsou 2 zařízení umožnují provoz v modu Active-Active
Musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	ANO	Je podporován režim HA v módu Active-Standby složený alespoň ze dvou zařízení
Musí podporovat rozšíření výkonu a kapacity zařízení (HA clusteru) pouze přidáním dalšího zařízení za pomoci externího load balanceru	ANO	Architektura podporuje rozšíření výkonu a kapacity zařízení (HA clusteru) pouze přidáním dalšího zařízení za pomoci externího load balanceru.
V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes NGFW	ANO	V rámci HA u firewallu Palo Alto jsou veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes NGFW
Musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy	ANO	High availibity mod umožnuje provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy

Obecné výkonové parametry:

Propustnost při plné aplikační kontrole musí dosahovat hodnoty alespoň 2,4 Gb/s (app mix)	ANO	Při plné aplikační kontrole je propustnost 2,6 Gbps
Propustnost při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 1 Gb/s (app mix)	ANO	propustnost při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV je 1.2 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 180 000	ANO	počet souběžných spojení je 200 000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 32 000	ANO	počet nových spojení za sekundu je 34 000

Síťová funkcionalita:		
Musí plně podporovat IPv4 i IPv6	ANO	Plná podpora pro IPv4 i IPv6
Musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	VPN koncetrátor obsahuje plná podporu pro zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP
Musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	VPN koncetrátor podporuje překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64
Musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)	ANO	Podporuje persistentní NAT pro DIPP (Dynamic IP and Port)
Musí podporovat VRF	ANO	Podporuje VRF
Musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	ANO	Podporuje směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)
Musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směřování	ANO	Plně podporuje MSDP (Multicast Source Discovery Protocol) pro pokročilé směřování
Musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směřování	ANO	Podporuje BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směřování
Musí podporovat nástroj pro pokročilé směřování (Advanced Routing Engine)	ANO	Podporuje nástroj pro pokročilé směřování (Advanced Routing Engine)
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel	ANO	PBR lze nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.
Musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let	ANO	Expirační dobu cookies lze nastavit v požadovaném intervalu (např na 1 až 5 let)

Musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury	ANO	VPN koncetrátor plně podporuje web proxy a umožnuje migraci proxy na NGFW beze změny architektury
Musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů	ANO	Podporuje stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů
Musí podporovat funkci DHCP serveru	ANO	Podporuje funkci DHCP serveru
Musí podporovat funkci DNS serveru/DNS Proxy	ANO	Podporuje funkci DNS serveru/DNS Proxy
Musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty	ANO	VPN koncetrátor umožnuje nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty
Musí umožnit nakonfigurovat IPSec tunnel s podporou post-quantum šifrování přímo na NGFW bez nutnosti použití třetích stran	ANO	VPN koncetrátor umožnuje nakonfigurovat IPSec tunnel s podporou post-quantum šifrování přímo na NGFW bez nutnosti použití třetích stran.
Musí podporovat výměnu hybridních post quantových klíčů založených na RFC 9242 a RFC 9370 v rámci IKEv2 a IPsec rekey	ANO	VPN koncetrátor (Firewall PA 440) podporuje výměnu hybridních post quantových klíčů založených na RFC 9242 a RFC 9370 v rámci IKEv2 a IPsec rekey
Musí podporovat vytváření hybridních post quantových klíčů použitím kryptografických sad NIST round 3 a round 4	ANO	VPN koncetrátor podporuje vytváření hybridních post quantových klíčů použitím kryptografických sad NIST round 3 a round 4
Musí podporovat na současně na jednom zařízení na úrovni síťového rozhraní konfigurace Span, Transparent, Layer 3 a Layer 2	ANO	Podporuje současně na jednom zařízení na úrovni síťového rozhraní konfigurace Span, Transparent, Layer 3 a Layer 2

VPN:		
Musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	ANO	Podporuje site-to-site VPN pomocí protokolu IPSec. Počet tunelů je licenčně neomezený
Musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2)	ANO	Plně podporuje Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2)
Počet současně připojených uživatelů nesmí být licenčně omezený	ANO	Počet současně připojených uživatelů není licenčně omezený
Musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS	ANO	Pro Remote Access VPN je poskytováno připojení z klientských operačních systémů Windows a macOS
Musí pro Remote Access VPN poskytovat připojení z mobilních operačních systémů Android a iOS	ANO	Pro Remote Access VPN je poskytováno připojení z mobilních operačních systémů Android a iOS

Musí pro Remote Access VPN poskytovat připojení z klientských a serverových operačních systémů Linux	ANO	Pro Remote Access VPN je poskytováno připojení z klientských a serverových operačních systémů Linux
Musí pro Remote Access VPN poskytovat připojení bez použití klienta pomocí webového portálu	ANO	Pro Remote Access VPN poskytuje připojení bez použití klienta pomocí webového portálu
Dodávané řešení musí obsahovat funkcionalitu kontroly připojovaných zařízení, která musí být v souladu s předdefinovanými podmínkami. Minimálně: verze OS, nainstalovaný antivirový nástroj, hodnota v registrech	ANO	V rámci nabízených VPN koncetrátorů PA-440 je zajištěna funkcionalita kontroly připojovaných zařízení, která musí být v souladu s předdefinovanými podmínkami. Podporováno - verze OS, nainstalovaný antivirový nástroj, hodnota v registrech.
Dodávané řešení musí umožnit přizpůsobení notifikace koncového uživatele o vypršení relace, aby se předešlo nechtěnému odhlášení	ANO	VPN koncetrátor umožnuje přizpůsobení notifikace koncového uživatele o vypršení relace, aby se předešlo nechtěnému odhlášení.
Propustnost IPSec musí být alespoň 1 Gb/s	ANO	Propustnost IPsec je 1,1 Gbps
Musí umožnovat vynucení aktualizace klientské VPN aplikace	ANO	Řešení umožnuje vynucení aktualizace klientské VPN aplikace
Musí podporovat Always-On VPN	ANO	Řešení podporuje Always-On VPN
Musí podporovat ověření uživatele v MS Active Directory, Radius	ANO	Řešení podporuje ověření uživatele v MS Active Directory, Radius
Musí podporovat ověření uživatele v MS Azure včetně MFA	ANO	Řešení podporuje ověření uživatele v MS Azure včetně MFA
Správa řešení:		
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru	ANO	Jednotlivé HW appliance obsahují plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru.
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management serveru	ANO	GUI podporuje čtení logových záznamů bez nutnosti používání centrálního management serveru.
Připojení ke GUI musí podporovat šifrování TLSv1.3	ANO	Připojení ke GUI podporuje šifrování TLSv1.3
GUI musí obsahovat offline kontextovou nápovědu	ANO	GUI obsahuje offline kontextovou nápovědu.
Musí být spravovatelný pomocí GUI nebo CLI přičemž GUI a CLI musí mít tzv. GUI. feature parity, poskytovat stejné možnosti konfigurace	ANO	VNP koncentrátor PaloAlto 440 je spravovatelný pomocí GUI nebo CLI přičemž GUI a CLI a obsahuje GUI. feature parity, poskytuje stejné možnosti konfigurace

Jednotlivé HW appliance musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování	ANO	Jednotlivé HW appliance obsahují plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI podporuje šifrování
Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování	ANO	Jednotlivé HW appliance obsahují plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.
Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku	ANO	Jednotlivé HW appliance umožnují automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku.
Musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	ANO	Řešení pro autentizaci a autorizaci administrátorů podporuje protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát
Musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	Obsahuje ativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu
Musí podporovat nativní nástroj pro odchycení provozu	ANO	Podporuje nativní nástroj pro odchycení provozu
Musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)	ANO	Řešení umožnuje spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)
NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	NGFW management podporuje práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem
Musí obsahovat funkci Policy Optimizer, která dokáže automaticky optimalizovat a migrovat L4 bezpečnostní politiku na L7 s identifikací aplikací	ANO	Obsahuje funkci Policy Optimizer, která dokáže automaticky optimalizovat a migrovat L4 bezpečnostní politiku na L7 s identifikací aplikací.
NGFW s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz	ANO	NGFW s novějšími verzemi OS umožnuje při při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz.
Nativní konfigurační rozhraní (API) NGFW musí podporovat standard OpenConfig bez nutnosti použití třetistranného nástroje	ANO	Nativní konfigurační rozhraní (API) NGFW podporuje standard OpenConfig bez nutnosti použití třetistranného nástroje.

Aplikační kontrola:

Musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	VPN koncetrátor má plnou podporu pro aplikační detekci a kontrolu jako svou nativní funkcionalitu
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	V rámci aplikační kontroly umožnuje přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	Definovaná aplikace představuje "match kritérium" při policy lookup
Musí podporovat identifikaci aplikací napříč všemi porty/protokoly	ANO	Plně podporuje identifikaci aplikací napříč všemi porty/protokoly
Musí podporovat identifikaci aplikací na nestandardních portech	ANO	Plně podporuje identifikaci aplikací na nestandardních portech
Identifikace aplikace musí probíhat přímo v NGFW	ANO	Identifikace aplikace probíhá přímo v NGFW
Musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	ANO	VPN koncentrátor Palo Alto 440 umožnuje detekci a zabrání aplikaci měnit porty, tzv. port-hopping
Musí podporovat řízení neznámého provozu	ANO	Plně podporuje řízení neznámého provozu
Musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	VPN koncentrátor Palo Alto 440 umožnuje tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Musí umožnovat zakázat instalaci nových signatur aplikací z aktualizací poskytovaných výrobcem	ANO	Umožnuje zakázat instalaci nových signatur aplikací z aktualizací poskytovaných výrobcem
Musí umožnovat odložení instalace nových signatur aplikací z aktualizací poskytovaných výrobcem	ANO	Umožnuje odložení instalace nových signatur aplikací z aktualizací poskytovaných výrobcem

Kontrola na úrovni uživatelských identit:		
Musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	Plně podporuje vytváření bezpečnostních pravidel na základě uživatelských identit
Musí umožnit blokování použití korporátní identity (kombinace login a heslo) uživatele v externích službách a aplikacích mimo organizaci	ANO	Umožnuje blokování použití korporátní identity (kombinace login a heslo) uživatele v externích službách a aplikacích mimo organizaci.
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	Volba uživatelské identity je nativní součástí vytváření standardního bezpečnostního pravidla
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	Uživatelská identita představuje "match kritérium" při policy lookup

Musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence	ANO	Umožnuje automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence
Musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení
Musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér
Musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance
Musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
Musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog
Musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)
Musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal
Musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno z VPN agenta
Musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)
Musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček	ANO	Podporuje získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček
ZTNA funkcionalita musí být realizovatelná přímo na NGFW bez nutnosti instalace dalších komponent, které mají samostaný management	ANO	ZTNA funkcionalita je realizovatelná přímo na NGFW bez nutnosti instalace dalších komponent, které mají samostaný management.

3)

Musí podporovat službu, která dokáže konzistentně ověřovat a autorizovat všechny uživatele bez ohledu na umístění a místo uložení identity uživatele (místní, cloudové nebo hybridní). Podpora autentifikačních a autorizačních mechanismů SAML a OpenID Connect	ANO	Podporuje službu, která dokáže konzistentně ověřovat a autorizovat všechny uživatele bez ohledu na umístění a místo uložení identity uživatele (místní, cloudové nebo hybridní). Je podporována autentifikačních a autorizačních mechanismů SAML a OpenID Connect.
NGFW řešení musí umožňovat redistribuci identit uživatelů z NGFW, kde je uživatel autentifikován na ostatní NGFW bez nutnosti instalace dalších komponent, které mají samostaný management	ANO	NGFW řešení umožnuje redistribuci identit uživatelů z NGFW, kde je uživatel autentifikován na ostatní NGFW bez nutnosti instalace dalších komponent, které mají samostaný management.
Musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná	ANO	Podporuje kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná
Dešifrování:		
Musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	Podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům
Musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	Podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru
Musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace	ANO	Podporuje dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace
Dešifrovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	ANO	Splňje podle požadavku - dešifrovaný provoz lze o definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita
Musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	Podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
Musí podporovat dešifrování protokolu TLS verze 1.3	ANO	Podporuje dešifrování protokolu TLS verze 1.3
Musí podporovat OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy	ANO	Podpororuje OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy
Ochrana proti DoS:		

Musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita	ANO	VPN koncenrátor obsahuje nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita
QoS:		
Musí poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)	ANO	Poskytuje možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)
Musí podporovat prioritizaci provozu na základě DSCP	ANO	Podporuje prioritizaci provozu na základě DSCP
Musí podporovat prioritizaci provozu na základě Identifikované aplikace	ANO	Podporuje prioritizaci provozu na základě Identifikované aplikace
Logování a reportování:		
Musí obsahovat lokální úložiště logů	ANO	VPN koncentrátor obsahuje lokální úložiště logů
Musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	VPN koncentrátor obsahuje nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI
Musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL	ANO	Podporuje agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL
Musí podporovat přeposílání logů na zařízení třetích stran	ANO	Podporuje přeposílání logů na zařízení třetích stran
Musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	Umožnuje výběr přeposílaných logů na úrovni bezpečnostního pravidla
Přeposílané logy z NGFW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	ANO	Přeposílané logy z NGFW jsou automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)
Musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní NGFW	ANO	Umožnuje vytváření vlastních reportů přímo z grafického rozhraní NGFW
Bezpečnostní funkcionality:		

Musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	Podporuje zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu
Musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve NGFW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	Obsahuje integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur je uložena přímo ve NGFW. Aplikace IPS profilu je granulární, na úrovni bezpečnostního pravidla
Musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	Umožnuje tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve NGFW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	Obsahuje integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur Musí být uložena přímo ve NGFW. Aplikace AV profilu Musí být granulární, na úrovni bezpečnostního pravidla
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	Antivirus umí kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB
Musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	Umožnuje tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
Musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	Plně podporuje možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci
Musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	V bezpečnostních pravidlech podporuje použití externích dynamických seznamů; poskytuje možnost ověřit na základě certifikátů pravost těchto dynamických seznamů
Musí podporovat import SNORT signatur manuálně a přes API	ANO	Podporuje import SNORT signatur manuálně a přes API.
Musí pro přístup ke kritickým aplikacím, poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci; tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla	ANO	Pro přístup ke kritickým aplikacím, poskytuje možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci; tato vlastnost je konfigurovatelná na úrovní bezpečnostního pravidla

Musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	Poskytuje možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu
Musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane	ANO	Podporuje analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane.
Musí umět zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení	ANO	Umí zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení.
Musí podporovat Local Deep Learning, který poskytuje mechanismus pro provádění rychlé, lokální analýzy zero-day a dalších vyhýbavých hrozeb založené na hlubokém učení	ANO	Podporuje Local Deep Learning, který poskytuje mechanismus pro provádění rychlé, lokální analýzy zero-day a dalších vyhýbavých hrozeb založené na hlubokém učení.
Musí být schopen odhalit a zablokovat neznámou C2 (Command&Controll) komunikaci (např. CobaltStrike, Empire), na kterou neexistuje detekční vzorek (signatura)	ANO	VPN koncentrátor je schopen odhalit a zablokovat neznámou C2 (Command&Controll) komunikaci (např. CobaltStrike, Empire), na kterou neexistuje detekční vzorek (signatura).
Detekce nezámé komunikace musí být realizovány přímo na NGFW bez nutnosti použití aktualizovaných IPS vzorků	ANO	Detekce nezámé komunikace jsou realizovány přímo na NGFW bez nutnosti použití aktualizovaných IPS vzorků.
Musí obsahovat lokální ML modely, které v případě detekce podezřelé komunikace odkloní tento provoz do cloudové služby pro pokročilou analýzu pomocí ML a Deep Learning	ANO	Obsahuje lokální ML modely, které v případě detekce podezřelé komunikace odkloní tento provoz do cloudové služby pro pokročilou analýzu pomocí ML a Deep Learning.
Musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách	ANO	Umožnuje tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.
Musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	Podporuje vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele
Řešení musí podporovat rozšíření funkcionality NGFW o bezpečnost IoT nativní (automatizovaná identifikace zařízení a jejich zranitelností, automatizovaná bezpečnostní pravidla pro IoT) bez nutnosti integrace s třetími stranami	ANO	Řešení podporuje rozšíření funkcionality NGFW o bezpečnost IoT nativní (automatizovaná identifikace zařízení a jejich zranitelností, automatizovaná bezpečnostní pravidla pro IoT) bez nutnosti integrace s třetími stranami.
Řešení musí podporovat rozšíření funkcionality NGFW o bezpečnost IoT nativní bez nutnosti instalace agentů nebo síťových sond	ANO	Řešení podporuje rozšíření funkcionality NGFW o bezpečnost IoT nativní bez nutnosti instalace agentů nebo síťových sond.

AI Access Security:		
Musí být rozšiřitelný o ochranu přístupu ke GenAI/LLM službám a aplikacím, ochrana musí být přímo dostupná na zařízení a nesmí být dodáná jako samostatné řešení	ANO	Lze rozšířit o ochranu přístupu ke GenAI/LLM službám a aplikacím, ochrana je přímo dostupná na zařízení a nebude dodáná jako samostatné řešení.

Podpora 2FA:		
Musí podporovat: přístupový komerční certifikát vydaný NCA, privátní klíč uložený na čipové kartě Starcos 3.7 C3, middleware SecureStore 8.0.1. a vyšší, čtečka čipových karet ACS	ANO	Nabízený VPN koncentrátor Palo Alto 440 podporuje přístupový komerční certifikát vydaný NCA, privátní klíč uložený na čipové kartě Starcos 3.7 C3, middleware SecureStore 8.0.1. a vyšší, včetně čtečky čipových karet ACS

Servisní podpora a licenční plán:		
Musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	Nabízený VPN koncentrátor Palo Alto 440 podporuje licenční model, který je nezávislý na počtu ochraňovaných koncových systémů
Požadovaná délka podpory a platnosti všech dodaných licencí je 60 měsíců	ANO	VPN koncetrátor bude dodán s délkou podpory a platnosti všech dodaných licencí je 60 měsíců
Nabízené řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware	ANO	Nabízené řešení není v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce jsou v době podání nabídky součástí stabilní verze operačního systému/firmware
Instalace na místě u zákazníka, konfigurace dle podmínek v místě a čase, respektování stávající síťové konfigurace a segmentace, podrobné zaškolení ke správě, ovládání i obslužnému centrálnímu management software	ANO	Součástí dodávky jsou veškeré činnosti- instalace na místě u zákazníka, konfigurace dle podmínek v místě a čase, respektování stávající síťové konfigurace a segmentace, podrobné zaškolení ke správě, ovládání i obslužnému centrálnímu management software
Servisní středisko: lokalizované v ČR, servisní technici se vzájemnou zastupitelností	ANO	Splňuje požadavek na servisní středisko: lokalizované v ČR, servisní technici se vzájemnou zastupitelností
Reakční doba technika: maximálně 48 hodin, komunikace v českém jazyce	ANO	Součástí nabízeného řešení je SLA - reakční doba technika: do 48 hodin, komunikace v českém jazyce