SMLOUVA
„POŘÍZENÍ, IMPLEMENTACE A PODPORA FIREWALLŮ“

uzavřená podle § 1746 odst. 2 a § 2358 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“) a zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorský zákon**“)

Název/Firma:	TresTech s.r.o.
Sídlo:	Hlubočepská 1291/2, 152 00 Praha 5
IČ:	04262719
Zapsán v OR:	Městský soud v Praze, sp. zn. C 244853
Zastupující:	Tomáš Hauzner, jednatel
Bankovní spojení:	Raiffeisenbank a.s., č. ú. 11403841/5500

(dále jen **„poskytovatel“** nebo **„smluvní strana“**)

a

Název/Firma:	**Agentura pro podporu podnikání a investic CzechInvest**
Sídlo:	Štěpánská 567/15, 120 00 Praha 2
IČ:	71377999
Zastupující:	Mgr. Ing. Jan Michal, generální ředitel

(dále jen **„objednatel“** nebo **„smluvní strana“**)

(oba společně dále jen **„smluvní strany“**)

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu (dále jen **„Smlouva“**).

PREAMBULE

Tato Smlouva se uzavírá na základě výsledku zadávacího řízení na nadlimitní veřejnou zakázku s názvem „**Pořízení, implementace a podpora firewallů**“ (dále jen „Veřejná zakázka“), ev č. VZ ve Věstníku veřejných zakázek Z2025-035022.

Poskytovatel bere na vědomí, že objednatel je správcem několika významných informačních systémů ve smyslu § 3 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, které splňují určující kritéria podle § 3 vyhlášky Národního bezpečnostního úřadu č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů.

Tato Veřejná zakázka je realizována v rámci projektu č. CZ.31.2.0/0.0/0.0/23_094/0010191, *Podpora a zajištění kybernetické bezpečnosti v rámci organizace CzechInvest*, který je součástí Národního plánu obnovy, komponenty 1.2 Digitální systémy veřejné správy, financovaného z EU Nástroje pro oživení a odolnost.

Poskytovatel prohlašuje, že:

a) ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**insolvenční zákon**“), a zavazuje se objednatele bezodkladně informovat o všech skutečnostech o hrozícím úpadku, popř. o prohlášení úpadku jeho společnosti, stejně jako o změnách v jeho kvalifikaci, kterou prokázal v rámci své nabídky na plnění veřejné zakázky v dále uvedeném smyslu; a
b) splňuje veškeré podmínky a požadavky stanovené v této Smlouvě a v zadávacích podmínkách, je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené a

c) disponuje odbornými schopnostmi, technickými prostředky a veškerými oprávněními nezbytnými k zajištění řádného poskytování služeb dle této Smlouvy; a

d) je ve smyslu ust. § 5 odst. 1 občanského zákoníku schopen při plnění této Smlouvy jednat se znalostí a pečlivostí, která je s jeho povoláním nebo stavem spojena, s tím, že případné jeho jednání bez této odborné péče půjde k jeho tíži. Poskytovatel nesmí svou kvalitu odborníka ani své hospodářské postavení zneužít k vytváření nebo k využití závislosti slabší strany a k dosažení zřejmé a nedůvodné nerovnováhy ve vzájemných právech a povinnostech smluvních stran, a

e) bere na vědomí, že se svou účastí ve veřejné zakázce hlásí jako příslušník určitého stavu nebo povolání k odbornému výkonu nebo jinak vystupuje jako odborník a dle ust. § 2950 občanského zákoníku tak nahradí škodu, způsobí-li ji neúplnou nebo nesprávnou informací nebo škodlivou radou danou za odměnu v záležitosti svého vědění nebo dovednosti, a

f) bere na vědomí, že objednatel není ve vztahu k předmětu této Smlouvy podnikatelem, a

g) disponuje veškerými odbornými předpoklady potřebnými pro poskytnutí služeb dle Smlouvy, je k jeho plnění oprávněn a na jeho straně neexistují žádné překážky, které by mu bránily plnění dle této Smlouvy objednateli poskytnout.

ČLÁNEK 1
PŘEDMĚT SMLOUVY

1.1 Předmětem Smlouvy je závazek poskytovatele na své náklady dodat firewallové řešení do prostředí objednatele (dále jen „firewallové řešení“) včetně jeho kompletní instalace a implementace v infrastruktuře objednatele a podpory, to vše po dobu 5 let, a závazek objednatele poskytnout poskytovateli součinnost nezbytnou k řádnému a včasnému plnění této Smlouvy, dále řádně poskytnuté plnění podle této Smlouvy od poskytovatele převzít a zaplatit mu za něj cenu sjednanou ve výši a za podmínek uvedených v této Smlouvě. Rozsah plnění podle této Smlouvy je vymezen v následujících odstavcích tohoto článku a v Příloze č. 1 k této Smlouvě.

1.2 Firewallové řešení

V rámci plnění Smlouvy budou dodány 2 ks perimetrových firewallů a 2 ks interních segmentačních firewallů splňujícího požadavky uvedené v Příloze č. 1 k této Smlouvě.

1.3 Implementační služby

V rámci plnění Smlouvy budou poskytnuty implementační služby zahrnující:

- analýzu prostředí objednatele a návrh řešení implementace,
- instalaci veškerého HW v prostředí objednatele
- implementaci a konfiguraci firewallového řešení,
- vytvoření a předání dokumentace,
- zaškolení administrátorů objednatele,
- testování provozu.

1.4 Služby podpory

V rámci plnění Smlouvy budou poskytovány služby servisní podpory, které zahrnují:

- eskalaci na support výrobce,
- přístup k aktualizacím a upgradům (OS, firmware, nové verze SW, upgrade SW a update všech bezpečnostních databází),
- Záruku na hardware formou výměny následující pracovní den (NBD),
- přístup do portálu výrobce (registrace zařízení, licencí, tahování updatů a upgradů, správa licencí).

ČLÁNEK 2
DOBA, MÍSTO A PODMÍNKY PLNĚNÍ

2.1 Poskytovatel se zavazuje dodat firewallové řešení v rozsahu podle čl. 1 odst. 1.2 této Smlouvy a dokončit implementační služby v rozsahu podle čl. 1 odst. 1.3 této Smlouvy do 90 (slovy: „devadesáti“) kalendářních dnů ode dne účinnosti této Smlouvy.

2.2 Poskytovatel se zavazuje poskytovat podporu firewallového řešení podle čl. 1 odst. 1.4 této Smlouvy po dobu 5 let ode dne předání implementovaného firewallového řešení.

2.3 Místem odevzdání a převzetí implementovaného firewallového řešení podle čl. 1 odst. 1.2 a 1.3 této Smlouvy je sídlo objednatele uvedené v záhlaví této Smlouvy (dále jen „**místo převzetí**“).

2.4 Za řádné poskytnutí dílčího plnění spočívající v dodávce a implementace firewallového řešení se považuje dodávka plnění podle čl. 1 odst. 1.2 této Smlouvy a zajištění implementačních služeb v rozsahu podle čl. 1 odst. 1.3 této Smlouvy, a to v termínu uvedeném v odst. 2.1 tohoto článku. O řádném dodání implementovaného firewallového řešení a po předvedení způsobilosti firewallového řešení sloužit svému účelu, tj. předvedení požadovaných funkcionalit podle Přílohy č. 1 k této Smlouvě, bude sepsán Akceptační protokol, který bude podepsán oprávněnými osobami obou smluvních stran.

Akceptační protokol předá poskytovatel objednateli nejpozději při odevzdání v místě převzetí a bude obsahovat tyto náležitosti:

- stručný popis firewallového řešení;
- potvrzení o poskytnutí případných licencí;
- stručný popis poskytnutých implementačních služeb;
- datum vystavení Akceptačního protokolu a podpis oprávněné osoby poskytovatele;
- podpis oprávněné osoby objednatele společně s uvedením data podpisu.

2.5 Objednatel je povinen implementované firewallové řešení převzít jen v případě, že odpovídá této Smlouvě, nejpozději však do 14 (slovy: „čtrnácti“) kalendářních dnů ode dne dokončení implementačních služeb, ledaže firewallové řešení má jakékoliv vady nebo nedostatky, nebo pokud Akceptační protokol neobsahuje veškeré náležitosti uvedené výše. Objednatel je povinen specifikovat v Akceptačním protokolu důvody, pro které jej odmítl podepsat, a stanovit náhradní termín ke splnění.

2.6 Služby podpory podle čl. 1 odst. 1.4 této Smlouvy, budou poskytovány ode dne následujícího po podpisu Akceptačního protokolu, kterým bude potvrzeno řádné dodání a zprovoznění předmětu plnění smlouvy. Služby budou fakturovány po částech, formou ročních období (dvanáctiměsíčních). První období začíná dnem následujícím po podpisu Akceptačního protokolu a trvá 12 měsíců.

ČLÁNEK 3
CENA

3.1 Poskytovateli náleží za řádné a úplné splnění předmětu Smlouvy splňujícího všechny požadavky podle této Smlouvy celková cena ve výši 10 950 909,00 Kč + DPH ve výši 2 299 690,89 Kč; cena včetně příslušné výše DPH činí 13 250 599,89 Kč.

Celková cena zahrnuje tyto jednotlivé dílčí částky:

3.1.1 Poskytovateli náleží za řádné dodání firewallového řešení podle čl. 1 odst. 1.2 této Smlouvy cena ve výši 6 945 254,00 Kč + DPH ve výši 1 458 503,34 Kč; cena včetně příslušné výše DPH činí 8 403 757,34 Kč.

3.1.2 Poskytovateli náleží za řádně poskytnuté implementační služby podle čl. 1 odst. 1.3 této Smlouvy cena ve výši 366 000,00 Kč + DPH ve výši 76 860,00 Kč; cena včetně příslušné výše DPH činí 442 860,00 Kč.

3.1.3 Poskytovateli náleží za řádně poskytované služby podpory podle čl. 1 odst. 1.4 této Smlouvy cena ve výši 727 931,00 Kč + DPH ve výši 152 865,51 Kč; cena včetně příslušné výše DPH činí 880 796,51 Kč za 1 rok poskytovaných služeb (dále jen „Roční poplatek"), tedy celková cena za období 5 let ve výši 3 639 655,00 Kč + DPH ve výši 764 327,55 Kč, cena vč. příslušné DPH činí 4 403 982,55 Kč za 5 let poskytovaných služeb.

3.2 Cena podle čl. 3 odst. 3.1 této Smlouvy obsahuje veškeré náklady a výdaje poskytovatele nutné k plnění této Smlouvy.

3.3 Změna ceny podle čl. 3 odst. 3.1 této Smlouvy je možná pouze v případě, pokud při realizaci předmětu plnění dojde ke změnám sazeb DPH. V tomto případě se cena upraví podle výše sazby DPH platné v době vzniku zdanitelného plnění, v takovém případě nebude vyhotoven dodatek k této Smlouvě a účinnost této změny nastává v návaznosti na účinnost změny příslušného obecně závazného právního předpisu.

ČLÁNEK 4
PLATEBNÍ PODMÍNKY

4.1 Objednatel uhradí příslušnou cenu podle čl. 3 odst. 3.1.1, 3.1.2 a 3.1.3 této Smlouvy na základě faktury, kterou poskytovatel vystaví a doručí objednateli nejpozději do 10 (slovy: „deseti") kalendářních dní po řádném poskytnutí implementačních služeb podle čl. 1 odst. 1.3 této Smlouvy, což bude stvrzeno podepsáním Akceptačního protokolu za podmínek čl. 2 odst. 2.4 této Smlouvy.

4.2 Poskytovatel je oprávněn fakturovat Roční poplatek za služby podpory podle čl. 3 odst. 3.1.3 této smlouvy vždy předem za každý 1 (slovy: „jeden") kalendářní rok, v němž mají být poskytovány služby podle čl. 1 odst. 1.4 této smlouvy, a to nejpozději do posledního dne měsíce předcházejícího počátku příslušného období poskytování služeb.

4.3 Příslušné ceny uhradí objednatel formou bezhotovostního převodu na účet poskytovatele uvedený v záhlaví této Smlouvy.

4.4 Každá faktura musí obsahovat odkaz na tuto Smlouvu a případě faktury za dodávku a implementaci firewallového řešení podle čl. 3 odst. 3.1.1 a 3.1.2 v příloze také kopii oboustranně podepsaného Akceptačního protokolu. Dále musí faktury obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku. Dále musí faktura obsahovat následující text: „*Tato zakázka je realizována v rámci projektu č. CZ.31.2.0/0.0/0.0/23_094/0010191, Podpora a zajištění kybernetické bezpečnosti v rámci organizace CzechInvest, který je součástí Národního plánu obnovy, komponenty 1.2 Digitální systémy veřejné správy, financovaného z EU Nástroje pro oživení a odolnost.*" V případě, že faktura doručená objednateli nebude obsahovat některou z předepsaných náležitostí, nebo ji bude obsahovat chybně, je objednatel oprávněn vrátit tuto fakturu poskytovateli. Lhůta splatnosti se v takovém případě přerušuje a počíná znovu běžet až od vystavení opravené či doplněné faktury.

4.5 Nebude-li jakákoli faktura splňovat veškeré výše uvedené náležitosti daňového dokladu, nebo bude-li mít jiné závady v obsahu, je objednatel oprávněn ji ve lhůtě její splatnosti poskytovateli vrátit a poskytovatel je povinen vystavit a doručit objednateli fakturu opravenou či doplněnou. V případě vrácení faktury dle předcházející věty se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku až dnem následujícím po dni, kdy byla opravená nebo doplněná faktura splňující všechny náležitosti dle příslušných právních předpisů a požadavky dle této Smlouvy, doručena objednateli.

4.6 Splatnost každé faktury činí 30 (slovy: „třicet") kalendářních dní a počítá se ode dne doručení faktury objednateli. Smluvní strany se dohodly, že dnem úhrady se rozumí den odepsání fakturované částky z účtu objednatele. Objednatel není v prodlení, uhradí-li fakturu 30 (slovy: „třicet") kalendářních dní po jejím obdržení, byť úhrada proběhne po termínu, který je na faktuře uveden jako den splatnosti.

4.7 Poskytovatel se zavazuje do 3 (slovy: „tří") kalendářních dnů po nabytí účinnosti této Smlouvy poskytnout objednateli písemné potvrzení správce daně o své registraci k dani z přidané hodnoty.

4.8 V případě, že se poskytovatel stane nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, je povinna o tom neprodleně písemně

informovat objednatele. Bude-li poskytovatel ke dni uskutečnění zdanitelného plnění veden jako nespolehlivý plátce, bude část ceny odpovídající dani z přidané hodnoty uhrazena přímo na účet správce daně v souladu s ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. O tuto částku bude ponížena celková cena a poskytovatel obdrží cenu bez DPH. V případě, že se poskytovatel stane nespolehlivým plátcem ve smyslu tohoto odstavce, má objednatel současně právo od této Smlouvy odstoupit.

ČLÁNEK 5
PRÁVA OBJEDNATELE PŘI OHROŽENÍ NEBO PORUŠENÍ LICENCE A PRÁVA Z VADNÉHO PLNĚNÍ POSKYTOVATELE

5.1 V případě, že dojde k ohrožení nebo porušení licencí, jsou-li poskytnuty v rámci plnění této Smlouvy objednateli, zavazuje se poskytovatel je plně ochránit a zprostit objednatele jakýchkoliv nároků třetích stran uplatňujících jakákoliv práva, včetně majetkových autorských práv vůči objednateli; utrpí-li objednatel v souvislosti s uplatněním nároků třetích stran jakoukoli škodu nebo nemajetkovou újmu, je poskytovatel povinen objednateli nahradit škodu a vypořádat vzniklou nemajetkovou újmu objednatele. Poskytovatel odpovídá za to, že předmět Smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, a že bude odpovídat technickým a bezpečnostním předpisům.

5.2 Práva objednatele z vadného plnění poskytovatele se podřizují dikci podle § 2099 až § 2117 občanského zákoníku. Objednatel je oprávněn oznámit poskytovateli vady poskytovaného plnění bez zbytečného odkladu poté, kdy byly nebo mohly být zjištěny při vynaložení odborné péče. Objednatel písemně oznámí vadu a/nebo uvede způsob, jakým se vada projevuje, a současně uplatní nárok. Poskytovatel se zavazuje, že vadu odstraní nejpozději do 2 (slovy: „dvou“) pracovních dnů po doručení oznámení objednatele.

5.3 Poskytovatel výslovně odpovídá za to, že dodané a implementované firewallové řešení dle této Smlouvy, případně jeho části, bude mít ke dni předání a převzetí jeho implementace objednatelem vlastnosti požadované objednatelem v této Smlouvě, resp. v Příloze č. 1 k této smlouvě a bude způsobilé k užití k účelu sjednanému touto Smlouvou. Poskytovatel výslovně prohlašuje, že plněním této Smlouvy neporušuje žádná autorská práva ani jiná vlastnická práva žádné třetí strany.

5.4 Neodstraní-li poskytovatel reklamované vady ve lhůtě sjednané v odst. 5.2 této Smlouvy je objednatel oprávněn pověřit odstraněním reklamované vady jinou odborně způsobilou právnickou nebo fyzickou osobu. Veškeré takto vzniklé náklady uhradí poskytovatel do 14 dnů ode dne, kdy obdržel písemnou výzvu objednatele k uhrazení těchto nákladů. Uhrazením nákladů na odstranění vad jinou odborně způsobilou osobou podle tohoto odstavce není dotčeno právo objednatele požadovat po poskytovateli náhradu vzniklé škody.

ČLÁNEK 6
MLČENLIVOST

6.1 Není-li dále stanoveno jinak, je poskytovatel povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví v souvislosti s plněním této Smlouvy. Tento závazek se rovněž vztahuje na veškeré informace, které objednatel předá poskytovateli a na veškeré skutečnosti, se kterými se poskytovatel seznámí při plnění této Smlouvy, zejména skutečnosti tvořící předmět obchodního tajemství nebo důvěrné informace (dále jen **„chráněné informace**“).

6.2 Závazek mlčenlivosti je poskytovatel povinen zajistit mimo jiné tím, že bez předchozího písemného souhlasu objednatele nedojde k jakémukoli šíření chráněných informací, anebo jejich zpřístupnění třetím osobám.

6.3 Závazek mlčenlivosti je poskytovatel povinen zachovávat jak po dobu plnění předmětu této Smlouvy, tak po jejím dokončení; tohoto závazku jej může zprostit pouze objednatel svým písemným prohlášením.

6.4 Poskytovatel je povinen zajistit, že chráněné informace budou přístupné pouze zaměstnancům a/nebo jiným osobám, které se budou podílet na plnění předmětu této Smlouvy (dále jen „**oprávněné osoby**“). Na vyžádání objednatele je poskytovatel povinen neprodleně objednateli poskytnout úplný seznam oprávněných osob (jméno a příjmení u fyzických osob a obchodní firmu a identifikační číslo u právnických osob).

6.5 Poskytovatel je povinen zajistit splnění závazku mlčenlivosti ve stejném rozsahu u oprávněných osob, a to tak, aby oprávněné osoby byly tímto závazkem vázány i po skončení pracovněprávního nebo jiného smluvního vztahu k poskytovateli.

ČLÁNEK 7
SMLUVNÍ POKUTA

7.1 Pokud bude poskytovatel v prodlení s plněním jakéhokoli závazku dle této Smlouvy, je objednatel oprávněn požadovat, aby poskytovatel zaplatil za každý započatý den prodlení smluvní pokutu ve výši 5.000,- Kč (slovy: „pět tisíc korun českých“).

7.2 V případě porušení závazku poskytovatele v rozsahu poskytovaných služeb specifikovaných v odst. 1.4 této Smlouvy, je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každé jednotlivé porušení.

7.3 V případě porušení závazku mlčenlivosti poskytovatele dle této Smlouvy, je poskytovatel povinen zaplatit objednateli smluvní pokutu ve výši 100.000,- Kč (slovy: „sto tisíc korun českých“) za každý jednotlivý případ porušení závazku.

7.4 Smluvní strany se dohodly, že smluvní pokuta je splatná 15. (slovy: „patnáctý“) kalendářní den od doručení písemné výzvy objednatele k její úhradě poskytovatelem.

7.5 Uplatněním nároku na smluvní pokuty objednatelem ani úhradou kterékoli smluvní pokuty poskytovatelem není dotčeno právo objednatele na náhradu škody nebo vypořádání nemajetkové újmy.

ČLÁNEK 8
ZÁNIK SMLOUVY

8.1 Smlouva zaniká vedle případů stanovených občanským zákoníkem také písemnou dohodou smluvních stran, v jejímž obsahu bude dohodnuto též vypořádání dosavadních vzájemných závazků smluvních stran, dále písemným odstoupením od Smlouvy objednatelem pro její podstatné porušení poskytovatelem vymezené níže, přičemž odstoupení od Smlouvy je účinné okamžikem doručení písemného oznámení objednatele o odstoupení poskytovateli.

8.2 V případě, že bude poskytovatel v prodlení s plněním kteréhokoli závazku této Smlouvy delším než 20 (slovy: „dvacet“) kalendářních dní, má se za to, že se jedná o podstatné porušení smluvní povinnosti ze strany poskytovatele, jež zakládá právo objednatele odstoupit od Smlouvy.

8.3 Objednatel je dále oprávněn odstoupit od Smlouvy v případě, že na majetek poskytovatele je vedeno insolvenční řízení nebo byl insolvenční návrh zamítnut pro nedostatek majetku poskytovatele, či poskytovatel vstoupí do likvidace. Objednatel je dále oprávněn odstoupit od Smlouvy z důvodů uvedených občanským zákoníkem (zejm. § 2001 a násl.).

8.4 Účinky odstoupení od Smlouvy se netýkají smluvních povinností souvisejících s povinností mlčenlivosti a povinností hradit jednotlivé smluvní pokuty, úroku z prodlení, pokud již dospěl do dne odstoupení, nároku na náhradu škody, vypořádání smluvních stran po odstoupení ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany po odstoupení.

ČLÁNEK 9
LICENCE A KOMUNIKACE

9.1 Poskytovatel poskytuje touto Smlouvou objednateli podporu užívání licence, je-li součástí předmětu plnění, v souladu čl. 1 odst. 1.2 této Smlouvy.

9.2 Poskytovatel touto Smlouvou neposkytuje objednateli oprávnění k rozmnožování, rozšiřování, pronájmu, půjčování, vystavování produktů, jež jsou součástí předmětu plnění této Smlouvy.

9.3 Poskytované licence, jež jsou součástí předmětu plnění této Smlouvy, jsou nevýhradní.

9.4 Veškeré úkony v souvislosti se vznikem, změnou nebo zánikem závazků plynoucích z této Smlouvy musí mít písemnou formu a musí být podepsány osobou oprávněnou jednat jménem příslušné smluvní strany a doručovány prostřednictvím datové schránky, doporučenou poštou nebo osobně.

9.5 Smluvní strany se dohodly, že (i) doručování provádějí na adresy / datové schránky uvedené v záhlaví této Smlouvy nebo v případě adresáta – poskytovatele, na doručovací adresu poskytovatele, která byla oznámena v souladu s čl. 11 odst. 11.10 této Smlouvy a (ii) obstarají řádné přijímání zásilek.

9.6 V případě, že smluvní strana odmítne převzít zásilku doručovanou provozovatelem poštovních služeb, nebo jinak vědomě zmaří její doručení, má se za to, že odmítnutí převzetí zásilky nebo zmaření doručení je dnem jejího doručení. V případě, že smluvní strana nevyzvedne zásilku v úložní době u provozovatele poštovních služeb, má se za to, že zásilka byla doručena třetím pracovním dnem od uložení.

9.7 Sdělení, příkazy, požadavky, výzvy, potvrzení a ostatní úkony týkající se plnění závazků z této Smlouvy se zavazují smluvní strany činit písemně prostřednictvím datových schránek, provozovatele poštovních (kurýrních) služeb nebo prostřednictvím e-mailové komunikace kontaktních osob smluvních stran:

Za poskytovatele: xxxxxx, xxxxxx, xxxxxx@trestech.cz

Za objednatele: xxxxx, xxxxxx, xxxxx@czechinvest.gov.cz

V případě změny v osobě kontaktní osoby informuje jedna smluvní strana druhou zprávou doručenou do datové schránky.

ČLÁNEK 10
UVEŘEJNĚNÍ UZAVŘENÉ SMLOUVY

10.1 Smluvní strany prohlašují a stvrzují svým podpisem uvedeným níže, že žádné ustanovení této Smlouvy nepodléhá obchodnímu tajemství dle § 504 občanského zákoníku, ani neobsahuje důvěrnou informaci o poměrech smluvní strany nebo skutečnostech, které má smluvní strana potřebu ochraňovat jako důvěrnou informaci nebo předmět obchodního tajemství.

10.2 Poskytovatel bere na vědomí povinnost uveřejnění obsahu této Smlouvy, změny Smlouvy (v podobě uzavřeného smluvního dodatku) podle povinností stanovených zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů, (dále jen „**zákon o registru smluv**“). Poskytovatel je srozuměn se zveřejněním této Smlouvy na profilu objednatele, budou-li naplněny požadavky zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

10.3 Splnění zákonné povinnosti v rozsahu podle § 5 odst. 1 zákona o registru smluv provede objednatel bez zbytečného odkladu po jejím uzavření. Objednatel prostřednictvím e-mailu neprodleně informuje poskytovatele o uveřejnění této Smlouvy v registru smluv, případně předá poskytovateli doklad o uveřejnění Smlouvy v registru smluv jako potvrzení skutečnosti, že Smlouva nabyla účinnosti.

10.4 Poskytovatel bere na vědomí, že objednatel je povinen zpřístupnit obsah této Smlouvy na základě dalších právních předpisů.

ČLÁNEK 11
ZÁVĚREČNÁ USTANOVENÍ

11.1 Objednatel si vyhrazuje právo na prodloužení plnění dle článku 1.4. Smlouvy, a to na dobu až 12 měsíců.

11.2 Smluvní strany se dohodly, že (i) poskytovatel není oprávněn postoupit Smlouvu, práva a závazky nebo pohledávky z této Smlouvy na třetí osobu, (ii) započtení pohledávky poskytovatele proti pohledávce objednatele lze pouze po dohodě smluvních stran a za podmínek stanovených příslušným právním předpisem.

11.3 Poskytovatel je povinen poskytnout Objednateli veškerou potřebnou součinnost a spolupůsobit při výkonu finanční kontroly dle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění. Poskytovatel musí umožnit kontrolu plnění podmínek poskytnutí podpory všem relevantním orgánům, zejména poskytovateli podpory (Ministerstvo vnitra), Ministerstvu financí, Nejvyššímu kontrolnímu úřadu, a dále i orgánům Evropské unie, zejména Evropské komisi, Evropskému účetnímu dvoru a OLAF.

11.4 Objednatel i Poskytovatel musí dodržovat zásady ochrany finančních zájmů EU, vyplývající především z Nařízení 2018/1046, kterým se stanoví finanční pravidla pro souhrnný rozpočet Evropské Unie (dále jen „**Finanční nařízení**“) a Nařízení 2021/241 stanovují nepřekročitelný rámec pro provádění RRF, k předcházení podvodům, korupci, dvojímu financování a střetu zájmů a jejich odhalování a nápravě.

11.5 Osoby, jejichž prostřednictvím Poskytovatel prokazoval způsobilost nebo kvalifikaci ve Veřejné zakázce, je Poskytovatel povinen využívat při plnění této Smlouvy, a to po celou dobu jejího trvání a lze je vyměnit pouze s předchozím písemným souhlasem Objednatele, který může být dán výlučně za předpokladu, že tyto osoby budou nahrazeny osobami splňujícími způsobilost nebo kvalifikaci požadovanou ve Veřejné zakázce. Poskytovatel je povinen poskytnout součinnost k tomu, aby byl Objednatel schopen identifikovat osoby poskytující plnění na jeho straně.

11.6 Osoby Objednatele i Poskytovatele se zdrží jakéhokoli jednání, které by mohlo uvést jejich zájmy do střetu se zájmy Evropské unie. Rovněž jsou povinny přijmout taková opatření, která u funkcí v rámci jejich odpovědnosti zamezí vzniku střetu zájmů a která řeší situace, jež lze objektivně vnímat jako střet zájmů. Ke střetu zájmů dochází, je-li z rodinných důvodů, z důvodů citových vazeb, z důvodů politické nebo národní sprízněnosti, z důvodu hospodářského zájmu nebo z důvodů jiného přímého či nepřímého osobního zájmu ohrožen nestranný a objektivní výkon funkcí účastníka finančních operací nebo jiné osoby dle čl. 61 Finančního nařízení. Na objednatele i poskytovatele se vztahuje informační povinnost tak, aby mohlo být odhaleno případné ohrožení finančních zájmů Unie s ohledem na aplikaci střetu zájmů dle čl. 61 Finančního nařízení.

11.7 Smluvní strany jsou si vědomy, že na realizaci plnění dle této Smlouvy není možné čerpat jinou veřejnou podporu podle článku 107 odst. 1 Smlouvy o fungování Evropské unie, podporu z prostředků Evropské unie, které centrálně spravují orgány, agentury, společné podniky a jiné subjekty Evropské unie a která není přímo ani nepřímo pod kontrolou členských států, a ani podporu v režimu de minimis. Nelze tedy čerpat podporu z jiného programu NPO nebo nástroje Evropské unie, případně od téhož poskytovatele dotace, ani z jiného programu nebo ze státního rozpočtu a dalších veřejných zdrojů. V případě zapojení dalšího typu podpory, bude poskytovatel objednatele o této skutečnosti neprodleně informovat a předloží příslušný právní akt, kterým byla podpora přiznána.

11.8 Jestliže se ukáže jakékoliv ustanovení nebo ujednání této Smlouvy jako neplatné nebo nevymahatelné nebo právně neúčinné, nedotýká se to ostatních ujednání nebo ustanovení této Smlouvy, a to za předpokladu, že ostatní ujednání Smlouvy jsou od neplatného, nevymahatelného nebo právně neúčinného ustanovení Smlouvy oddělitelná. Smluvní strany se zavazují, že takové ustanovení nebo ujednání nahradí platným, účinným a vymahatelným ustanovením nebo ujednáním, které má stejný nebo obdobný smysl nebo účinek a učiní tak do 15 (slovy: „patnácti“) pracovních dnů ode dne doručení výzvy jedné smluvní strany druhé smluvní straně.

11.9 Tato Smlouva a veškeré mimosmluvní závazky vyplývající z této Smlouvy se řídí a vykládají v souladu s právem České republiky, zejména občanským zákoníkem. Použití dispozitivních ustanovení právních předpisů je však vyloučeno v rozsahu, ve kterém by mohlo měnit kterékoliv ujednání nebo

ustanovení této Smlouvy, či význam, účel nebo interpretaci kteréhokoliv ujednání nebo ustanovení této Smlouvy.

11.10 Smluvní strany se zavazují, že budou postupovat v souladu s oprávněnými zájmy druhé smluvní strany, a že uskuteční veškerá právní jednání, která se ukáží být nezbytná pro realizaci závazků upravených touto Smlouvou. Závazek součinnosti se vztahuje pouze na takové úkony, které přispějí či mají přispět k dosažení účelu této Smlouvy.

11.11 Veškeré změny a doplnění jednotlivých ujednání nebo ustanovení této Smlouvy mohou být provedeny pouze formou číslovaného písemného dodatku podepsaného oběma smluvními stranami a výslovně nazvaného dodatek ke Smlouvě, v případě změny sídla, místa podnikání, nebo doručovací adresy poskytovatele, je poskytovatel povinen neprodleně tuto skutečnost oznámit objednateli. Pokud poskytovatel tuto povinnost nesplní, platí pro doručování písemností adresa uvedená v záhlaví této Smlouvy.

11.12 Poskytovatel na sebe přebírá nebezpečí změny okolností podle § 1765 odst. 2 občanského zákoníku.

11.13 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

11.14 Nedílnou součástí této Smlouvy jsou přílohy:

- Příloha č. 1 – Požadavky na funkcionality a vlastnosti firewallového řešení
- Příloha č. 2 – Funkční specifikace nabízeného firewallového řešení
- Příloha č. 3 – Seznam členů realizačního týmu
- Příloha č. 4 – Seznam poddodavatelů

11.15 Tato Smlouva je podepsána vlastnoručně, nebo elektronicky. Je-li Smlouva podepsána vlastnoručně, je vyhotovena ve dvou (2) stejnopisech, z nichž každý bude považován za prvopis. Každá smluvní strana obdrží jeden (1) stejnopis této Smlouvy. Je-li tato Smlouva podepsána elektronicky, je podepsána pomocí uznávaného elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, osoby oprávněné jednat za smluvní stranu.

11.16 Smluvní strany prohlašují, že Smlouva byla uzavřena podle jejich vážné a svobodné vůle, že nejednají v omylu či tísni, Smlouvu si přečetly, považují obsah této Smlouvy za určitý a srozumitelný, jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této Smlouvy rozhodující, a na důkaz toho připojují ke Smlouvě své podpisy.

V……dne:…….2025	V Praze dne:…….2025
Za poskytovatele:	Za objednatele:
……..	……..
Tomáš Hauzner	Mgr. Ing. Jan Michal
jednatel	generální ředitel
TresTech s.r.o.	Agentura pro podporu podnikání a investic CzechInvest

PŘÍLOHA Č. 1

POŽADAVKY NA FUNKCIONALITY A VLASTNOSTI FIREWALLOVÉHO ŘEŠENÍ

1. Perimetrové firewally

HW požadavky

- musí se jednat o HW appliance (VM appliance ani SW řešení není akceptovatelné);
- cluster o dvou fyzických zařízeních, podpora režimu vysoké dostupnosti min. v režimu active/active a active/pasive;
- max. velikost 2 RU;
- redundantní napájení – 2 hot swap zdroje;
- min. 2x rozhraní 25GE SFP28;
- min. 6x optické datové rozhraní SFP+ o rychlosti 10Gb/s;
- min. 10x síťové rozhraní 1GE RJ45;
- management rozhraní 1 GE RJ45 a sériový konzolový port;
- integrovaný pevný disk SSD s celkovou kapacitou min. 2x240 GB (eventuálně 1x 480 GB) pro lokální úložiště provozních informací (logů).

Výkonové požadavky

- propustnost firewallu pro IPv4 provoz s analýzou aplikací min. 18 Gbps;
- počet současně navázaných spojení firewallu min. 2 000 000, počet nových spojení za sekundu min. 200 000;
- celková propustnost IPSEC VPN min. 9 Gbps;
- propustnost funkce IPS min. 9 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování);
- propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 10 Gbps.

Funkční požadavky

- grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů;
- bezpečnostní funkce obecně označované jako Next Generation firewall;
- systém honeypot pro detekci útoků přes protokol TCP s automatickou blokací komunikace útočníka do interní sítě s nastavitelným časovým omezením;
- možnost automatického sdílení bezpečnostních informací o kybernetických hrozbách v rámci kolektivního systému výrobce;
- napojení na alespoň 5 dalších bezpečnostních databází geograficky významných pro místo nasazení;
- multihoming (vícero konektivit) v režimu active-backup s možností definice serverů pro testování jednotlivých konektivit;
- podpora stavového firewallingu pro IPv4 i IPv6;
- možnost nasazení ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy, transparentní proxy (inline);
- plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster,

plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná);

- ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Kerberos), Single Sign On;
- podpora lokální databáze a vzdálené databáze pro ověřování uživatelů;
- podpora funkcí VPN brány
    - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran);
    - OpenVPN pro klientský přístup nebo SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup;
- podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3;
- funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak); podpora detekce a blokace stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod; podpora detekce/mitigace neznámých škodlivých vzorek přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu, nebo nutnosti instalace pluginů do prohlížeče;
- funkce kategorizace webových stránek (web filtering) s podporou minimálně kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze, pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, nutnost autentizace uživatele pro určitou kategorii;
- funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možnost definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, možnost importu SNORT signatur, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů;
- funkce 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;
- možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), data a času;
- podpora explicitní proxy s podporou konfiguračních PAC souborů pro režim nasazení explicitní proxy;
- analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), ochrana proti Domain Generation Algorythm (DGA), filtrování DNS dotazů na základě kategorizace;
- integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejmenší počet aktivních spojení) s podporou SSL inspekce pro rozkládaný provoz.

Další požadavky

- Součástí dodávky jsou licence na funkce Application Control, IPS, Anti-Virus, DNS inspekce a URL filteringu včetně aktualizací signatur z webu výrobce po celou dobu kontraktu.
- Součástí dodávky budou 4 ks 10 Gbps SFP+ transceiverů, multimode, short-range od výrobce shodného s výrobcem firewallu.

2. Interní segmentační firewally

HW požadavky

- musí se jednat o HW appliance (VM appliance ani SW řešení není akceptovatelné);
- cluster o dvou fyzických zařízeních, podpora režimu vysoké dostupnosti min. v režimu active/active a active/pasive;
- max. velikost 2 RU;
- redundantní napájení – 2 hot swap zdroje;
- min. 2x rozhraní 25GE SFP28;
- min. 10x optické datové rozhraní SFP+ o rychlosti 10Gb/s;
- min. 10x síťové rozhraní 1GE RJ45;
- management rozhraní 1 GE RJ45 a sériový konzolový port;
- integrovaný pevný disk SSD s celkovou kapacitou min. 2x240 GB (eventuálně 1x 480 GB) pro lokální úložiště provozních informací (logů).

Výkonové požadavky

- propustnost firewallu pro IPv4 provoz s analýzou aplikací min. 18 Gbps;
- počet současně navázaných spojení firewallu min. 2 000 000, počet nových spojení za sekundu min. 200 000;
- celková propustnost IPSEC VPN min. 9 Gbps;
- propustnost funkce IPS min. 9 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování);
- propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 10 Gbps.

Funkční požadavky

- grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů;
- bezpečnostní funkce obecně označovaných jako Next Generation firewall;
- podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – možnost rozšíření na min. 10 virtuálních kontextů; každý virtuální kontext musí pracovat izolovaně;
- podpora stavového firewallingu pro IPv4 i IPv6;
- možnost nasazení ve všech z následujících režimu (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy, transparentní proxy (inline);
- plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná);
- ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Kerberos) Single Sign On;
- podpora lokální databáze a vzdálené databáze pro ověřování uživatelů;
- podpora funkcí VPN brány
    - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran);
    - OpenVPN pro klientský přístup nebo SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup;
- podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3;
- funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě

IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak); podpora detekce a blokace stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod; podpora detekce neznámých vzorek přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu, nebo nutnosti instalace pluginů do prohlížeče;

- funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace;
- funkce kategorizace webových stránek (web filtering) s podporou kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, nutnost autentizace uživatele pro určitou kategorii;
- funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, možnost importu SNORT signatur, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů;
- funkce 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;
- možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), data a času;
- podpora explicitní proxy s podporou konfiguračních PAC souborů pro režim nasazení explicitní proxy;
- analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), ochrana proti Domain Generation Algorythm (DGA), filtrování DNS dotazů na základě kategorizace;
- Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejmenší počet aktivních spojení) s podporou SSL inspekce pro rozkládaný provoz.

VPN specifikace

- u VPN agenta na koncovém zařízení podpora operačních systémů min. Windows, MacOS, Android, iOS, Linux;
- integrace s Active Directory pro autentizaci uživatelů;
- schopnost pracovat s uživatelskými skupinami z Active Directory;
- VPN klient s podporou SSL VPN a IPsec VPN;
- možnost vytvářet vlastní instalační balíčky VPN klientů v rámci GUI;
- agent na klientském zařízení dokáže posílat telemetrická data o koncovém zařízení na management klientů;
- přiřazení "tagů" koncovým zařízení na základě telemetrických dat (nainstalovaný antivirový nástroj, hodnota v registrech. atd.) a práce s těmito tagy v politikách na FW;
- podpora ZTNA (Zero trust network access);
- možnost filtrovat provoz na konkrétní URL odkazy;
- schopnost vyčítat informace o softwaru a aplikacích nainstalovaných na koncových zařízeních.

Další požadavky

- Součástí dodávky jsou licence na funkce Application Control, IPS, Anti-Virus, DNS inspekce a URL filteringu včetně aktualizací signatur z webu výrobce po celou dobu kontraktu.
- Součástí dodávky bude 6 ks 10 Gbps SFP+ transceiverů, multimode, short-range od výrobce shodného s výrobcem firewallu.

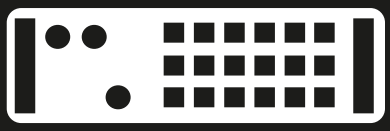
PŘÍLOHA Č. 2

FUNKČNÍ SPECIFIKACE NABÍZENÉHO FIREWALLOVÉHO ŘEŠENÍ

Přílohu (specsheet/datasheet) přiloží zadavatel před podpisem Smlouvy s vybraným dodavatelem dle jeho nabídky

KERNUN

KSA-440-LHE



Váš **expertní partner** v kybersvětě

KERNUN Security Appliance v sobě obsahuje to nejlepší z našich produktů vyladěné k vaší spokojenosti. Jedná se o **komplexní produkt**, který umožňuje integraci tří balíčků zaměřených na jednotlivé otázky **zabezpečení síťového provozu**. Můžete si tak vybrat řešení přesně na míru vašim potřebám

Base package – základní balíček

- Nastavení síťování, segmentace sítě, bezpečné připojení do interní sítě
- **Využijete pro** bezpečné propojení poboček, zabezpečené připojování zaměstnanců do interní sítě

IP security package – rozšiřující balíček

- Silné zabezpečení síťové infrastruktury
- **Využijete pro** ochranu před aktivními hrozbami na základě vyhodnocování podezřelých IP adres

Web gateway package – rozšiřující balíček

- Řízení přístupu na web z interní sítě
- **Využijete pro** ochranu uživatelů před nežádoucím obsahem, řízení webového provozu zaměstnanců

20+
let
s Vámi na
trhu

100+
zákazníků
nám
důvěřuje

5000+
zařízení
pomáháme
chránit

KERNUN, a.s.
Ptašínského 309/6
602 00 Brno
IČO: 26239701
Tel: +420 545 423 160
E-mail: info@kernun.cz

Technické parametry

Základní parametry	
Provedení	2U Rack instalace
Procesor	AMD, EPYC 7203
RAM	32 GB
Uložiště	2 TB, SSD
Management	IPMI s dedikovaným LAN portem

Síťová rozhraní	
25 GbE	4x
10 GbE	12x
1 GbE	14x

Propustnost zařízení	
Propustnost firewallu	20 Gbps
Propustnost IPS	11 Gbps
Současně otevřených spojení	2 500 000
Nově otevřených spojení	250 000 / s
Propustnost IPsec VPN	11 Gbps
Propustnost NGFW funkcí	10 Gbps

Co s námi získáte?

- **Firmu s tradicí** orientovanou na dlouhodobou spokojenost svých zákazníků
- **Kvalitní produkt** na míru vašim potřebám
- **Podporu v češtině**, která je zkušená, ochotná a expertní
- **Dodavatele i výrobce**, který všem svým produktům skutečně rozumí
- **Stále aktuální informace** o rizicích na českém internetu
- **Automatickou ochranu**, kterou nemusíte hlídat

PA-3400 Series — Datasheet

Hlavní přednosti

• První ML-Powered Next-Generation Firewall (NGFW) na světě.

• Jedenáctkrát po sobě lídr v Gartner Magic Quadrant pro Network Firewalls.

• Lídr ve Forrester Wave: Enterprise Firewalls, Q4 2022.

• Rozšiřuje viditelnost a bezpečnost na všechna zařízení, včetně neřízených IoT, bez nutnosti nasadit další senzory.

• Nativní podpora web proxy v NGFW pro zjednodušení a konsolidaci správy funkcí firewallu a proxy.

• Podporuje vysokou dostupnost v režimech active/active i active/passive.

• Dodává předvídatelný výkon i se zapnutými bezpečnostními službami.

• Podporuje centralizovanou správu pomocí Panorama® network security management.

• Maximalizuje investice do bezpečnosti a předchází výpadkům podnikání se Strata™ Cloud Manager.

PA-3400 Series

Palo Alto Networks PA-3400 Series ML-Powered NGFW zahrnuje modely PA-3440, PA-3430, PA-3420 a PA-3410; cílené na nasazení jako vysokorychlostní internetové brány. Zařízení řady PA-3400 zabezpečují veškerý provoz.

První ML-Powered Next-Generation Firewall (NGFW) na světě umožňuje předcházet neznámým hrozbám, vidět a chránit vše — včetně Internet of Things (IoT) — a snižovat chyby díky automatickým doporučením politik.

Řídicí prvek řady PA-3400 je PAN-OS®, stejný software, který běží na všech NGFW Palo Alto Networks. PAN-OS nativně klasifikuje veškerý provoz — aplikace, hrozby a obsah — a váže jej na uživatele bez ohledu na umístění nebo typ zařízení. Aplikace, obsah a uživatelé — prvky, na nichž stojí vaše podnikání — tvoří základ bezpečnostních politik, což zlepšuje bezpečnostní postoj a zkracuje dobu reakce na incident.

Klíčové bezpečnostní a konektivitní funkce

ML-Powered Next-Generation Firewall

• Vkládá strojové učení (ML) do jádra firewallu a poskytuje inline bezsignaturní prevenci útoků pro souborové útoky a okamžitě zastavuje dosud neznámé phishingové pokusy.

• Využívá cloudové ML procesy pro doručení podpisů a instrukcí bez zpoždění zpět do NGFW.

• Používá behaviorální analýzu k detekci IoT zařízení a poskytuje doporučení politik; jde o cloudově doručovanou a nativně integrovanou službu v NGFW.

• Automatizuje doporučení politik, čímž šetří čas a snižuje riziko lidské chyby.

Identifikace a kategorizace všech aplikací na všech portech, kdykoliv (plná inspekce L7)

• Identifikuje aplikace v síti bez ohledu na port, protokol, vyhýbavé techniky nebo šifrování (SSL/TLS); s předplatným SaaS Security navíc automaticky objevuje a řídí nové aplikace, aby držel krok s explozí SaaS.

• Používá aplikaci — nikoliv port — jako základ pro rozhodnutí politik bezpečného zpřístupnění: povolit, zamítnout, plánovat, inspektovat a tvarovat provoz.

• Umožňuje vytvářet vlastní App-ID™ tagy pro proprietární aplikace nebo požádat Palo Alto Networks o vývoj App-ID pro nové aplikace.

• Identifikuje veškerá data v rámci aplikace (např. soubory a datové vzory) a blokuje škodlivé soubory a pokusy o exfiltraci dat.

• Vytváří standardní i přizpůsobené reporty o používání aplikací, včetně SaaS reportů s přehledem o schváleném i neschváleném SaaS provozu ve vaší síti.

• Umožňuje bezpečnou migraci starých L4 pravidel na pravidla založená na App-ID díky integrovanému Policy Optimizeru — pravidla jsou bezpečnější a snáze spravovatelná.

Více v technickém přehledu App-ID: App-ID Tech Brief

Prosazení bezpečnosti pro uživatelská zařízení kdekoli s adaptivními politikami

• Zajišťuje viditelnost, politiky, reportování a forenzní analýzy podle uživatelů a skupin — nikoli pouze IP adres.

• Snadno se integruje s širokou škálou úložišť informací o uživatelích: bezdrátové LAN kontroléry, VPN, adresářové servery, SIEM, proxy aj.

• Umožňuje definovat Dynamic User Groups (DUG) na firewallu a provádět časově omezené bezpečnostní akce bez čekání na změny v adresářích.

• Aplikuje konzistentní politiky bez ohledu na umístění uživatelů (kancelář, domov, cesty) a zařízení (iOS/Android; macOS/Windows/Linux; Citrix/Microsoft VDI; terminálové servery).

• Zabraňuje úniku firemních přihlašovacích údajů na weby třetích stran a brání opakovanému použití odcizených přihlašovacích údajů zavedením MFA na síťové vrstvě pro libovolnou aplikaci bez změn aplikace.

• Poskytuje dynamické bezpečnostní akce na základě chování uživatelů pro omezení podezřelých či škodlivých uživatelů.

• Umožňuje důsledně autentizovat a autorizovat uživatele bez ohledu na umístění a umístění identitních úložišť; pomáhá přejít k Zero Trust díky Cloud Identity Engine — zcela nové cloudové architektuře pro bezpečnost založenou na identitě.

Více v přehledu řešení Cloud Identity Engine: Cloud Identity Engine Solution Brief

Prevence škodlivé aktivity skryté v šifrovaném provozu

• Inspektuje a aplikuje politiky na šifrovaný SSL/TLS provoz, příchozí i odchozí, včetně TLS 1.3 a HTTP/2.

• Nabízí bohatou viditelnost do TLS provozu (objem šifrovaného provozu, verze SSL/TLS, sady šifer aj.) bez dešifrování.

• Umožňuje kontrolu nad využíváním zastaralých TLS protokolů, nezabezpečených šifer a špatně nakonfigurovaných certifikátů.

• Usnadňuje nasazení dešifrování a umožňuje využít vestavěné logy pro řešení problémů (např. aplikace s pinned certifikáty).

• Umožňuje flexibilně povolit/zakázat dešifrování dle kategorie URL, zdrojové/cílové zóny, adresy, uživatele, skupiny, zařízení a portu — pro potřeby ochrany soukromí a regulací.

• Umožňuje vytvořit kopii dešifrovaného provozu z firewallu (decryption mirroring) a poslat jej do nástrojů pro forenzní analýzu, historii nebo DLP.

• Umožňuje inteligentně přeposílat veškerý provoz (dešifrovaný TLS, ne-dešifrovaný TLS i ne-TLS) do nástrojů třetích stran pomocí network packet brokeru, optimalizovat výkon sítě a snížit provozní náklady.

Více o dešifrování v whitepaperu: Decryption — Why, Where and How

AI-powered sjednocená správa a provoz se Strata™ Cloud Manager

• Předcházejte přerušením sítě: prediktivní analýzy odhadnou stav nasazení a až 7 dní dopředu odhalí kapacitní úzká hrdla; proaktivně tak předejdete provozním výpadkům.

• Posilujte bezpečnost v reálném čase: analýza politik poháněná AI a průběžné kontroly shody s oborovými i doporučeními Palo Alto Networks.

• Umožněte NetSec správu a provoz: snadná správa konfigurací a bezpečnostních politik napříč všemi form-faktory (SASE, HW/SW firewally) a všemi bezpečnostními službami; zajistíte tak konzistenci a snížíte provozní režii.

Nativní podpora web proxy v Next-Generation Firewallu

• Konsolidace firewallu a proxy do jedné platformy se správou na centrální platformě (tvorba politik).

• Podpora explicitní proxy pomocí PAC souborů i transparentní proxy.

• Explicitní proxy pomáhá s architekturami bez default route v on-premise nasazeních proxy.

• Explicitní proxy podporuje autentizaci přes Kerberos a SAML.

• Transparentní proxy zjednodušuje nasazení bez nutnosti WCCP a autentizace.

Cloud-delivered Security Services (Precision AI®)

Útočná plocha podniků se s hybridní prací, cloudem, IoT a SaaS výrazně rozšířila a hrozby se rychle stupňují. Cloud-delivered Security Services přinášejí špičkové zabezpečení v reálném čase pro uživatele, zařízení i data — kdekoli.

Služby využívají Precision AI inline, sdílené informace o hrozbách od více než 70 000 zákazníků po celém světě a nativní integraci s NGFW a SASE pro eliminaci mezer a jednotnou správu.

• Advanced Threat Prevention: Zastavuje známé i neznámé exploity, malware, spyware a C2 hrozby — včetně až o 60 % více injekčních útoků a o 48 % více vysoce vyhýbavého C2 provozu než tradiční IPS; přináší průmyslově první prevenci zero-day útoků.

• Advanced WildFire®: Zajišťuje bezpečný přístup k souborům díky největšímu enginu prevence malwaru v odvětví; zastaví až o 22 % více neznámého malwaru a promění detekci v prevenci až 180× rychleji než konkurence.

• Advanced URL Filtering: Zajišťuje bezpečný přístup na web a zabrání až o 40 % více hrozbám v reálném čase než tradiční databáze; jako první v odvětví předchází známým i neznámým phishingovým útokům, zastaví až 88 % škodlivých URL nejméně 48 hodin před konkurencí.

• Advanced DNS Security: Chraňte DNS provoz a zastavujte pokročilé DNS vrstvé hrozby v reálném čase, včetně DNS hijackingu; pokrytí DNS hrozeb je 2× větší než u konkurence.

• Next-Generation CASB: Objevte a řiďte veškerou spotřebu SaaS (viditelnost do 60k+ SaaS aplikací) a chraňte data s 28+ API integracemi.

• IoT Security: Zabezpečte slepá místa a chraňte každé připojené zařízení jedinečné pro váš obor; objeví 90 % zařízení do 48 hodin — nejkomplexnější Zero Trust pro IoT.

Jedinečné zpracování paketů: Single-Pass Architecture

• V jednom průchodu provádí směrování, vyhledání politik, dekódování aplikací a porovnávání signatur pro všechny hrozby a obsah; významně snižuje procesní režii při konsolidaci více funkcí do jednoho bezpečnostního zařízení.

• Nezavádí latenci: prohledává provoz na všechny signatury v jednom průchodu pomocí stream-based, jednotného porovnávání signatur.

• Umožňuje konzistentní a předvídatelný výkon i při zapnutých bezpečnostních předplatných (propustnost Threat Prevention měřena s více předplatnými zapnutými).

SD-WAN funkcionalita

• Snadné přijetí SD-WAN — stačí ji povolit na stávajících firewallech.

• Bezpečné nasazení SD-WAN díky nativní integraci s naším špičkovým zabezpečením.

• Výjimečná uživatelská zkušenost díky minimalizaci latence, jitteru a ztrát paketů.

Výkon a kapacity PA-3400 Series

	PA-3410	**PA-3420**	**PA-3430**	**PA-3440**
Firewallová propustnost (Appmix)*	14 Gbps	19 Gbps	29 Gbps	35 Gbps
Propustnost Threat Prevention (Appmix)†	7.5 Gbps	10 Gbps	15 Gbps	20 Gbps
IPsec VPN propustnost‡	6.6 Gbps	9.9 Gbps	12 Gbps	14.5 Gbps
Max. souběžné relace§	1.4M	2.2M	2.5M	3M
Nové relace za sekundu||	145,000	220,000	240,000	268,000
Virtuální systémy (základ/max)#	1/11	1/11	1/11	1/11

* Firewallová propustnost měřena s App-ID a logováním, využívá Appmix transakce.

† Propustnost Threat Prevention měřena s App-ID, IPS, antivirus, antispyware, WildFire, file blocking a logováním; využívá Appmix transakce.

‡ IPsec VPN propustnost měřena s 64 KB HTTP transakcemi a zapnutým logováním.

§ Max. souběžné relace měřeny na HTTP transakcích.

|| Nové relace/s měřeny s application override a 1-bytovými HTTP transakcemi.

Přidání virtuálních systémů nad základ vyžaduje samostatnou licenci.

Pozn.: Výsledky měřeny na PAN-OS 11.2.

Síťové funkce (Networking Features)

Režimy rozhraní: L2, L3, tap, virtual wire (transparentní režim).

Směrování: OSPFv2/v3 s graceful restart, BGP s graceful restart, RIP, statické směrování.

Policy-based forwarding.

PPPoE (Point-to-Point Protocol over Ethernet).

Multicast: PIM-SM, PIM-SSM, IGMP v1, v2 a v3.

BFD (Bidirectional Forwarding Detection).

IPsec a SSL VPN:

• Výměna klíčů: ruční klíč, IKEv1 a IKEv2 (pre-shared key, autentizace na základě certifikátu).

• Šifrování: 3DES, AES (128/192/256bit).

• Autentizace: MD5, SHA-1, SHA-256, SHA-384, SHA-512.

• GlobalProtect® large-scale VPN pro zjednodušenou konfiguraci a správu*.

• Zabezpečený přístup přes IPsec a SSL VPN tunely pomocí GlobalProtect Gateway a portálů*.

* Vyžaduje licenci GlobalProtect.

VLANy:

• 802.1Q VLAN tagy na zařízení/na rozhraní: 4 094 / 4 094.

• Agregovaná rozhraní (802.3ad), LACP.

NAT:

• Režimy NAT (IPv4): statická IP, Dynamic IP, Dynamic IP and Port (PAT).

• NAT64, NPTv6.

• Další funkce NAT: rezervace Dynamic IP, laditelná oversubskripce Dynamic IP and Port.

Vysoká dostupnost (High Availability):

• Režimy: active/active, active/passive, HA clustering.

• Detekce poruch: path monitoring, interface monitoring.

Mobilní síťová infrastruktura (PA-3440 a PA-3430):

• 5G Security.

• GTP Security.

• SCTP Security.

Další informace: ML-Powered NGFWs for 5G (datasheet)

Hardwarové specifikace

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)

Úložiště: 480 GB SSD.

Trusted Platform Module (TPM): Integrované pro secure boot, hardware root of trust a zabezpečení systémových tajemství.

Napájecí zdroj (prům./max. spotřeba): redundantní 450W AC (133 W / 190 W).

Max BTU/h: 650.

Vstupní napětí / frekvence: AC 100–240 VAC (50–60 Hz).

Max. proudový odběr: AC 1,9 A @ 100 VAC; 0,8 A @ 240 VAC.

MTBF: 22 let.

Rozměry pro rack montáž: 1U, 19" standard; 14.15" × 17.15" × 1.70".

Hmotnost (samostatně / při expedici): 15.5 lb / 25 lb.

Bezpečnostní certifikace: cTUVus, CB.

EMI: FCC Class A, CE Class A, VCCI Class A.

Certifikace: viz paloaltonetworks.com/company/certifications.html

Prostředí:

• Provozní teplota: 0–40 °C (32–104 °F).

• Skladovací teplota: –20–70 °C (–4–158 °F).

• Vlhkost: 10–90 %.

• Max. nadmořská výška: 3 048 m (10 000 ft).

• Směr proudění vzduchu: zepředu dozadu.

PŘÍLOHA Č. 3

SEZNAM ČLENŮ REALIZAČNÍHO TÝMU

JMÉNO A PŘÍJMENÍ	POZICE	TELEFON	E-MAIL
XXX	PROJEKTOVÝ MANAŽER	XXX	XXX@TRESTECH.CZ
XXX	TECHNIK PALO ALTO	XXX	XXX@TRESTECH.CZ
XXX	TECHNIK KERNUN	XXX	XXX@KERNUN.CZ

PŘÍLOHA Č. 4

SEZNAM PODDODAVATELŮ

Prohlašuji, že výše uvedený dodavatel provede veřejnou zakázku prostřednictvím následujících poddodavatelů:

	Identifikační údaje poddodavatele	Popis plnění, které bude poddodavatel zajišťovat	% podíl na plnění veřejné zakázky
1.	KERNUN, a.s. sídlo: Ptašínského 309/6, 602 00 Brno IČO: 26239701	Dodávka a implementace části plnění výrobce Kernun	30%

V Praze dne dle el. podpisu

Jméno, příjmení jednající osoby (jednajících osob): Tomáš Hauzner

.....

podpis