SMLOUVA O KOUPI A PODPOŘE

číslo Prodávajícího: SML/2024/185 **číslo Kupujícího: INV-2025-0003-0612**

Smluvní strany

Společnost	ALEF NULA, a.s
se sídlem:	Pernerova 691/42, 186 00 Praha 8 - Karlín
zastoupená:	Ing. Milanem Zinkem, předsedou představenstva
IČO:	61858579
DIČ:	CZ61858579
bankovní spojení:	Komerční banka, a.s. – CZK
číslo účtu:	51-3717150237/0100
kontaktní osoba:	
e-mail:	
ID datové schránky:	ft2cp8u

zapsaná v OR vedeném u Městského soudu v Praze, spisová značka B 2727

(dále jen „**Prodávající**“)

a

Český metrologický institut

se sídlem:	Okružní 31, 638 00 Brno
zastoupená:	Ondřejem Kebrlem, odborným ředitelem pro ekonomiku
IČO:	00177016
DIČ:	CZ00177016
bankovní spojení:	Česká národní banka
číslo účtu:	198139621/0710
pověřený pracovník:	
e-mail:	
ID datové schránky:	65msw6w

(dále jen „**Kupující**“)

(Prodávající a Kupující dále společně jako „**smluvní strany**“)

uzavřely níže uvedeného dne, měsíce a roku podle § 2079 a násl. a § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“),

tuto
smlouvu o koupi a podpoře

(dále jen „**smlouva**“)

I.

Úvodní ustanovení

Tato smlouva je smluvními stranami uzavřena na plnění veřejné zakázky zadávané v otevřeném řízení „Dodávka firewallů pro ČMI 2024“.

II.

Předmět plnění

1. Předmětem této smlouvy je dodávka zboží (dále též i „zařizení“) a služeb vymezených v Příloze č. 1 této smlouvy a specifikovaných v Příloze č. 2 této smlouvy Prodávajícím vč. dopravy zboží do místa plnění, instalace a zprovoznění zboží (HW) v místě plnění, záruky a poskytování podpory.
2. Kupující se zavazuje předmět plnění od prodávajícího převzít a zaplatit cenu mu stanovenou v této smlouvě.

III.

Celková cena

1. Smluvní strany se dohodly, že cena zboží a služeb dodávaných Prodávajícím na základě této smlouvy během prvních 5 let po dodání zboží byla stanovena v souladu s nabídkovou cenou Prodávajícího nabídnutou v rámci zadávacího řízení veřejné zakázky specifikované v této smlouvě a činí **8 327 289,50 Kč bez DPH** (slovy: osm-miliónů-tři-sta-dvacet-sedm-tisíc-dvě-stě-osmdesát-devět korun českých, 50/100), DPH 21 % činí 1 748 730,80 Kč, tj. 10 076 020,30 Kč (slovy: deset-miliónů-sedmdesát-šest-tisíc-dvacet korun českých, 30/100) včetně DPH.
2. Rozpis dílčích cen za jednotlivé položky plnění (za zboží a služby po dobu prvních 5 let po dodání zboží) je uveden v příloze č. 1 této smlouvy.
3. Ceny za služby po uplynutí 5 let od dodání zboží, bude-li mít Kupující o tyto služby nadále zájem, budou stanoveny takto:
   - Prodloužení záruky NBD On-site: cena bude stanovena dohodou na základě aktuální nabídky Prodávajícího, která se bude odvíjet od ceny záruky a podpory ze strany výrobce firewallů.
   - Následná standardní podpora: cena může být změněna dohodou, přičemž dohodnutá cena nesmí být vyšší než cena následné standardní podpory uvedená v příloze č. 1 této smlouvy pod položkou č. 4 navýšená o inflaci v souladu s následující inflační doložkou.

     Inflační doložka:

     Prodávající je oprávněn písemně navrhnout navýšení aktuálně platné ceny následné standardní podpory poprvé nejdříve 2 měsíce před ukončením 5leté podpory započaté po dodání zboží a následně 1x ročně vždy po vyhlášení průměrné roční míry inflace Českým statistickým úřadem za uplynulý rok.

     Navržené navýšení ceny nesmí překročit částku odpovídající součinu aktuálně platné ceny a součtu průměrných ročních inflací (v %) od data, kdy podle této smlouvy začala platit aktuálně platná cena.

Do součtu průměrných ročních inflací (v předchozí větě) se započítají inflace jen za ty roky, ve kterých trvalo poskytování podpory za aktuálně platnou cenu alespoň 8 měsíců.

Součástí návrhu Prodávajícího musí být výpočet max. možné částky navýšení dle výše uvedeného popisu a rovněž Prodávajícím navrhované navýšení.

Kupující se musí k navrženému navýšení ceny vyjádřit nejpozději do 30 dnů od data doručení návrhu.

4. Ceny bez DPH, uvedené v Příloze č. 1 této smlouvy, jsou považovány za ceny nejvýše přípustné a nepřekročitelné, zahrnující poplatky za autorská práva, celní poplatky, dopravy do míst plnění, instalace a zprovoznění zboží (HW) v místě plnění a poskytování podpory včetně dalších nákladů souvisejících s dodávkou předmětu plnění v této smlouvě výslovně neuvedených.
5. Ceny za služby dle odst. 3 tohoto článku nebo jejich změny mohou být stanoveny nebo upravovány pouze formou dodatků k této smlouvě.

IV.
Doba a místo plnění

1. Prodávající je povinen dodat smluvené zboží specifikované v této smlouvě nejpozději do 6 měsíců ode dne nabytí účinnosti této smlouvy.
2. Prodávající je povinen poskytovat po dodání zboží zvýšenou podporu a následnou podporu (definovanou v Příloze č. 2 této smlouvy) v pracovních dnech od 9:00 do 17:00 hodin na základě požadavku ze strany Kupujícího. Reakční doba a doba zahájení podpory ze strany Prodávajícího nesmí přesáhnout 2 hodiny od vznesení požadavku Kupujícího.
3. Místem plnění je Český metrologický institut, referát IT, Hvožďanská 2053/3, 148 00 Praha 4.

V.
Všeobecné dodací podmínky

1. Dodávka zboží dle této smlouvy bude považována za uskutečněnou jejím převzetím Kupujícím a podpisem dodacího listu zástupci Prodávajícího a Kupujícího v místě plnění. Jedno vyhotovení dodacího listu zůstane Kupujícímu a druhé vyhotovení bude předáno Prodávajícímu.
2. Kupující nabývá vlastnické právo k dodanému zboží jeho převzetím. Přechod nebezpečí škody na zboží se řídí ustanovením § 2121 a násl. OZ.
3. Každá dodávka zboží musí obsahovat dodací list, v němž jsou obsaženy údaje jen o aktuálně dodávaném zboží.
4. Prodávající je povinen zachovávat mlčenlivost o všech skutečnostech obchodní, výrobní či technické povahy souvisejících s Kupujícími, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu a nejsou v příslušných obchodních kruzích běžně dostupné. Prodávající je povinen zajistit mlčenlivost ve stejném rozsahu i u všech osob, které musí tyto skutečnosti k plnění této smlouvy znát, vůči třetím právnickým nebo fyzickým osobám.

5. Na daňovém dokladu – faktuře (dále jen „faktura“) a v dodacím listě Prodávající uvede **unikátní identifikační** číslo zboží, přiděleno výrobcem tohoto zboží, pokud toto číslo položka předmětu plnění, která je uvedena v Příloze č. 1 této smlouvy, obsahuje.

VI.
Technické a platební podmínky

1. Platba za uskutečněné dodávky zboží a souvisejících služeb, které jsou započítány do ceny položek č. 1 až 3 v Příloze č. 1 této smlouvy (doprava, 5 let záruky NBD On-site a 12 měsíců podpory), příp. položky 6 a následující, pokud jsou v Příloze č. 1 této smlouvy uvedeny, bude provedena bezhotovostním platebním převodem na základě faktury vystavené Prodávajícím do 21 kalendářních dnů po řádném předání a převzetí zboží Kupujícím. Přílohou faktury bude zástupci obou stran podepsaný dodací list potvrzující, že zboží bylo dodáno Kupujícímu v požadovaném množství a kvalitě.
2. Platby za následnou standardní podporu (za 2. až 5. rok, příp. za další roky) bude provedena bezhotovostním platebním převodem na základě faktur za roční podporu vystavených Prodávajícím 1x ročně, a to do 21 kalendářních dnů po začátku období, ve kterém bude tato podpora poskytována.
3. Faktury musí splňovat náležitosti zákona č. 235/2004 Sb., o dani z přidané hodnoty, § 11 zákona č. 563/1991 Sb., o účetnictví, a § 435 OZ, to vše ve znění pozdějších předpisů, obsahovat i evidenční číslo smlouvy Kupujícího. V případě, že faktura nebude obsahovat náležitosti stanovené zákonem a touto smlouvou nebo bude obsahovat chybné údaje, nebo nebude-li u faktury dle odst. 1 přiložen potvrzený dodací list, je Kupující oprávněn fakturu Prodávajícímu vrátit, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadné faktury Kupujícímu.
4. Faktury jsou splatné do 30 kalendářních dnů ode dne prokazatelného doručení faktury Kupujícímu na e-mailovou adresu  nebo na adresu uvedenou na titulní straně této smlouvy.
5. Cena plnění je považována za zaplacenou okamžikem odepsání příslušné finanční částky z účtu Kupujícího ve prospěch účtu Prodávajícího.
6. Platby budou provedeny vždy v české měně na základě předložené faktury, cena uvedená na faktuře bude dle matematických pravidel vždy zaokrouhlena na dvě desetinná místa.
7. Ceny budou uvedeny bez DPH. K ceně bude připočtena DPH dle zákonné sazby v době uskutečnění zdanitelného plnění. V případě Prodávajícího s účtem vedeným v zahraničí bude DPH vypočítáno a odvedeno podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
8. Zálohové platby Kupující neposkytuje.

VII.
Záruka

1. Prodávající je povinen dodat zboží v požadovaném množství, jakosti a balení ve sjednaných dodacích termínech.

2. Prodávající prohlašuje, že dodávané zboží bude odpovídat nárokům na jakost, obsaženým v příslušných normách a technické specifikaci jednotlivých položek uvedených v Příloze č. 2. Pokud to vyžadují obecně závazné předpisy, bude dodávané zboží vybaveno předepsaným dokladem, příp. dalšími požadavky stanovenými právními předpisy.

3. Na dodávky zboží bude poskytnuta Prodávajícím záruka za jakost, která zaručuje, že zboží bude odpovídat technické specifikaci stanovené v Příloze č. 2 této smlouvy a bude prosté právních vad. Prodávajícím bude na dodané zboží poskytnuta záruka v délce a parametrech stanovených v Příloze č. 2 této smlouvy. Záruka začíná běžet okamžikem převzetí zboží Kupujícím.

4. Vady, které Kupující zjistí až po převzetí zboží, je Prodávající povinen odstranit nejpozději do třiceti (30) kalendářních dnů od doručení reklamace. Prodávající odstraní vady bezúplatně dodáním náhradního plnění v množství, druhu a jakosti dle této smlouvy.

5. Jsou-li ve vadném zařízení instalována záznamová paměťová média (harddisk, paměťová karta, flashdisk apod.), na kterých by se mohly nacházet informace podléhající ochraně ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, bude zboží předáno k reklamaci vady bez těchto médií, aniž by tato skutečnost měla vliv na plnění ze záruky Prodávajícím. Bude-li vadné paměťové médium, je Prodávající povinen nahradit jej bezvadným, a to pouze na základě čestného prohlášení Kupujícího o tom, že paměťové zařízení není funkční. Vadný kus (paměťové médium) nebude Prodávajícímu v tomto případě vydán.

6. U reklamovaného zboží, u kterého byla reklamace uznána, a bylo vyměněno za bezvadné, běží nová záruční lhůta ode dne předání bezvadného zboží Kupujícímu.

7. Nebyla-li reklamace včas a řádně Prodávajícím vyřešena, má Kupující právo požadovat náhradu škody či újmy v souladu s příslušnými ustanoveními OZ.

8. Prodávající prohlašuje, že má uzavřenou pojistnou smlouvu s pojištěním odpovědnosti za škodu způsobenou třetí osobě při výkonu podnikatelské činnosti, a to s limitem pojistného plnění alespoň 500 000 Kč a spoluúčastí maximálně 5 % a toto pojištění bude udržovat po celou dobu trvání této smlouvy.

VIII.
Sankce

1. Prodávající je oprávněn požadovat na Kupujícím smluvní pokutu za nedodržení termínu splatnosti ceny zboží ve výši 0,05 % z oprávněně fakturované částky bez DPH za každý i započatý den prodlení. Výše sankce není omezena.

2. Kupující je oprávněn požadovat na Prodávajícím smluvní pokutu za nedodržení termínu plnění dodávky zboží, stanoveného v této smlouvě, a to ve výši 0,05 % z ceny nedodaného zboží bez DPH za každý i započatý den prodlení. Výše sankce není omezena.

3. Kupující je oprávněn požadovat na Prodávajícím smluvní pokutu za prodlení s poskytnutím podpory dle čl. IV. odst. 2 této smlouvy (dodržení doby reakce a

zahájení podpory 2 hodiny od vznesení požadavku), a to ve výši 500 Kč za každou započatou hodinu prodlení. Výše sankce za 1 den je omezena na 4000 Kč.

4. Kupující je oprávněn požadovat na Prodávajícím smluvní pokutu za nedodržení termínu doručení faktury dle čl. VI. odst. 1 a 2 této smlouvy (21 kalendářních dnů), a to ve výši 0,05 % z ceny uvedené na faktuře bez DPH za každý i započatý den prodlení. Výše sankce není omezena.
5. Kupující je oprávněn požadovat na Prodávajícím smluvní pokutu za nedodržení doby pro odstranění zjištěných vad na základě reklamace dle čl. VII odst. 4 této smlouvy (30 kalendářních dnů), a to ve výši 0,05 % z ceny reklamovaného zboží bez DPH, a to za každý i započatý den prodlení. Minimální výše sankce je 100 Kč za den.
6. Pro případ porušení povinnosti mlčenlivosti definované v čl. V. odst. 4. je Kupující oprávněn požadovat na Prodávajícím smluvní pokutu ve výši 50 000 Kč (slovy: padesát tisíc korun českých) za každé jednotlivé porušení povinnosti.
7. Smluvní pokuty jsou splatné do 30 kalendářních dnů od data, kdy byla povinné straně doručena písemná výzva k jejich zaplacení oprávněnou stranou, a to na účet oprávněné strany uvedený v písemné výzvě. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši.

IX.
Platnost a účinnost smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu obou smluvních stran a je uzavřena na dobu neurčitou.
2. Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.
3. Smluvní strany souhlasí s uveřejněním plného znění této smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), a rovněž na profilu Kupujícího, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění smlouvy prostřednictvím registru smluv zajistí Kupující.
4. Smluvní vztah založený touto smlouvou může být ukončen:
   a) Dohodou smluvních stran.
   b) Výpovědí kterékoliv ze stran s výpovědní lhůtou 1 (jeden) měsíc, která začne plynout prvního dne měsíce následujícího po měsíci doručení výpovědi druhé straně.

      Kupující však může smlouvu vypovědět nejdříve po 1 roce využívání podpory, tj. po 1 roce od dodání zboží (firewallů), Prodávající nejdříve po 5 letech od dodání zboží (firewallů).
   c) Odstoupením od smlouvy v souladu s ustanoveními § 2001 a násl. OZ a také z následujících důvodů:
      i. Kupující je oprávněn od této smlouvy odstoupit v případě podstatného porušení povinností Prodávajícím; za podstatné porušení povinností Prodávajícího se považuje prodlení s dodáním zboží (firewallů) delší než

2 (dva) měsíce nebo nedodání zboží v požadované kvalitě a množství dle této smlouvy.

ii. Kupující je oprávněn odstoupit od smlouvy, jestliže nabude právní moci rozhodnutí insolvenčního soudu, jímž se osvědčuje úpadek Prodávajícího dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

iii. Prodávající je oprávněn od této smlouvy odstoupit v případě podstatného porušení povinností Kupujícím; za podstatné porušení povinností Kupujícího se považuje prodlení s placením po dobu delší než patnáct (15) dní, které není odstraněno ani do patnácti (15) dnů ode dne doručení písemné výzvy Prodávajícího Kupujícímu k odstranění prodlení Kupujícího.

X.

Řešení sporů

1. Veškeré spory mezi smluvními stranami nebo mezi Prodávajícím a Kupujícím budou řešeny nejprve smírně.
2. Nebude-li smírného řešení v případě sporu mezi Prodávajícím a Kupujícím dosaženo, bude spor řešen příslušným soudem České republiky s místní příslušností dle sídla Kupujícího.

XI.
Odpovědnost za škody

1. Prodávající odpovídá za škodu způsobenou vadným plněním této smlouvy v rozsahu stanoveném příslušnými ustanoveními OZ.

XII.
Závěrečná ustanovení

1. Tato smlouva se řídí právním řádem České republiky, zejména příslušnými ustanoveními OZ.
2. Smlouva může být měněna nebo doplňována jen písemnými, očíslovanými dodatky podepsanými oběma smluvními stranami, které se stanou nedílnou součástí této smlouvy.
3. Obě smluvní strany prohlašují, že tato smlouva nebyla uzavřena v tísni, ani za jednostranně nevýhodných podmínek, a na důkaz toho připojují své elektronické podpisy.
4. Tato smlouva je vyhotovena pouze v elektronické podobě a elektronicky podepsána Prodávajícím a Kupujícím.
5. Nedílnou součástí této smlouvy jsou následující přílohy:

   Příloha č. 1: Předmět plnění a cena

Příloha č. 2: Specifikace zařízení a služeb

Příloha č. 3: Produktové listy k předmětu plnění

V Praze dne /viz datum el. podpisu/

Za Prodávajícího:

Ing. Milan Zinek
předseda představenstva

V Brně dne /viz datum el. podpisu/

Za Kupujícího:

Ondřej Kebrle, BBA, MSc.
Odborný ředitel pro ekonomiku

Příloha č. 1: Předmět plnění a cena

Příloha č. 1 smlouvy - Předmět plnění a cena

Číslo položky	Název položky	Počet	Měrná jednotka	Nabídková cena za jednotku bez DPH [Kč]	Sazba DPH	Nabídková cena za množství bez DPH	DPH za množství	Nabídková cena za množství s DPH	Výrobce *)	Model *)	Číslo modelu (Part Number) *)
1.	**Hlavní firewall**	4	Ks	884 564,20	21	3 538 256,81 Kč	743 033,93 Kč	4 281 290,73 Kč	Palo Alto Networks	1410	PAN-PA-1410
2.	**Výkonný pobočkový firewall**	5	Ks	395 625,14	21	1 978 125,69 Kč	415 406,40 Kč	2 393 532,09 Kč	Palo Alto Networks	455	PAN-PA-455
3.	**Standardní pobočkový firewall**	9	Ks	107 364,70	21	966 282,31 Kč	202 919,29 Kč	1 169 201,60 Kč	Palo Alto Networks	415	PAN-PA-415

*) U položek 1 až 3 - Dodavatel doplní do zeleně podbarvených buněk výrobce, model a číslo modelu nabízeného HW.

Pozn.: V nabídkové ceně za jednotku u položek č. 1 až 3 jsou kromě pořizovací ceny samotného firewallu zahrnuty následující související služby (detailní popis služeb je uveden v příloze č. 2 smlouvy):
- doprava do místa plnění
- Záruka NBD On-site na daný firewall po dobu 60 měsíců
- Zvýšená podpora při implementaci - certifikovaným administrátorem daného FW s praxí min 5 let u daného FW - po dobu 4 měsíců
- Následná standardní (poimplementační) podpora - certifikovaným administrátorem daného FW s praxí min 5 let u daného FW - po dobu 8 měsíců

(dohromady tedy je v ceně každé jednotky u položek č. 1 až 3 zahrnuta i doprava, 5 let záruky NBD On-site a 12 měsíců podpory, která bude poskytována bezprostředně po dodání firewalů do místa plnění)

Číslo položky	Název položky	Počet	Měrná jednotka	Nabídková cena za jednotku bez DPH [Kč]	Sazba DPH	Nabídková cena za množství bez DPH	DPH za množství	Nabídková cena za množství s DPH
4.	**Následná standardní podpora - certifikovaným administrátorem daného FW s praxí min 5 let u daného FW **)**	4	roky	100 000,00	21	400 000,00 Kč	84 000,00 Kč	484 000,00 Kč
5.	**Zaškolení Administrátorů pro správu FW - certifikovaným školitelem/ školicím centrem daného FW**	1	Ks	60 180,00	21	60 180,00 Kč	12 637,80 Kč	72 817,80 Kč

**) Následná standardní podpora (položka č. 4) začne být poskytována po ukončení podpory, která je zahrnuta v ceně položek č. 1. až 3, tzn. 12 měsíců po dodávce firewalů.

Číslo položky	Název položky ***)	Počet **)	Měrná jednotka	Nabídková cena za jednotku bez DPH [Kč]	Sazba DPH	Nabídková cena za množství bez DPH	DPH za množství	Nabídková cena za množství s DPH	Výrobce		Přesný název licence (produktu)
6.	**PAN-SFP-SX**	14	Ks	6 260,63	21	87 648,75 Kč	18 406,24 Kč	106 054,99 Kč	Palo Alto Networks		SFP form factor, SX 1Gb optical transceiver, 550m reach on OM2 MMF, duplex LC, IEEE 802.3z 1000BASE-SX compliant
7.	**PAN-SFP-PLUS-SR**	4	Ks	18 663,75	21	74 655,00 Kč	15 677,55 Kč	90 332,55 Kč	Palo Alto Networks		SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant
8.	**PAN-PA-1410-GP-5YR-HA2**	4	Ks	99 933,75	21	399 735,00 Kč	83 944,35 Kč	483 679,35 Kč	Palo Alto Networks		PA-1410, GlobalProtect subscription, for one (1) device in an HA pair, 5 years (60 months) term.
9.	**PAN-SFP-CG**	6	Ks	12 403,13	21	74 418,75 Kč	15 627,94 Kč	90 046,69 Kč	Palo Alto Networks		SFP form factor, 1Gb copper transceiver, 100m over Cat5 RJ-45, IEEE 802.3ab 1000BASE-T compliant
10.	**PAN-SOFTWARE-NGFW-CR (Standard)**	30	Ks	11 428,59	21	342 857,81 Kč	72 000,14 Kč	414 857,95 Kč	Palo Alto Networks		Software NGFW Credits to deploy VM-Series, CN-Series, Subscription Services, and Virtual Panorama to manage Software Firewalls.
11.	**PAN-PRA-25**	1	Ks	133 363,13	21	133 363,13 Kč	28 006,26 Kč	161 369,38 Kč	Palo Alto Networks		Panorama central management software, 25 devices
12.	**PAN-SVC-PREM-PRA-25-5YR**	1	Ks	271 766,25	21	271 766,25 Kč	57 070,91 Kč	328 837,16 Kč	Palo Alto Networks		Premium support 5 year term, Panorama 25 devices

***) Pokud u firewalů uvedených v pol. č. 1 až 3 je nutné pro zajištění všech funkcí a parametrů firewalů (uvedených v příloze č. 2 smlouvy) pořízení nějakých licencí, musí být zajištění těchto licencí součástí nabídky dodavatele. Dodavatel v tom případě uvede tyto licence jako položky č. 6, 7 ... atd. (do tabulky je možné přidat další řádky).

Celková cena bez DPH za dodávku, zaškolení, pětiletou záruku a pětiletou podporu:	**8 327 289,50 Kč**	
Celková cena s DPH za dodávku, zaškolení, pětiletou záruku a pětiletou podporu:		**10 076 020,30 Kč**

Příloha č. 2 smlouvy

Specifikace zařízení a služeb

A/ Specifikace zařízení

		Popis požadavku	Splněno (Ano/Ne)	Skutečná hodnota parametru zařízení nabízeného dodavatelem
Hlavní firewall				
Název zařízení-model:		**PAN-PA-1410**		
	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 a pod.. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW	ANO	
		Výrobce NGFW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls v posledním aktuálním reportu společnosti Gartner	ANO	
	Požadavky na HW architekturu:			
		NGFW musí být typu HW appliance	ANO	
		Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"	ANO	
		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	
		NGFW musí obsahovat alespoň jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	
		NGFW musí obsahovat minimálně 4 metalické datové rozhraní o rychlosti 1Gb/s a 4 SFP+ dátových rozhraní o rychlosti 10Gb/s	ANO	4xSPF/SFP+, 6xSFP,4xRJ45/PoE,8xRJ45
		NGFW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu NGFW	ANO	
		NGFW musí být schopen ukládat logové údaje na interní SSD disk o velikosti minimálně 120 GB	ANO	120 GB SSD
		NGFW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	
		NGFW musí být rozměrově kompatibilní s 19“ rozvaděčem	ANO	

NGFW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V	ANO	

Požadavky na High Availability (HA):		
NGFW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení	ANO	
NGFW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	ANO	
NGFW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti i v geograficky oddělených lokalitách	ANO	
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	
NGFW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy	ANO	

Obecné výkonové parametry:		
Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň 8,3 Gb/s (app mix)	ANO	8.5Gbps
Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 4 Gb/s (app mix)	ANO	4.5Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 940 000	ANO	945000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 100 000	ANO	100000

Síťová funkcionalita:		
NGFW musí plně podporovat IPv4 i IPv6	ANO	
NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	
NGFW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	
NGFW musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)	ANO	
NGFW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	ANO	
NGFW musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směřování.	ANO	
NGFW musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směřování.	ANO	
NGFW musí podporovat nástroj pro pokročilé směřování (Advanced Routing Engine)	ANO	
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	
NGFW musí podporovat napájení PoE (Power Over Ethernet) na připojená síťová zařízení	ANO	

NGFW musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let	ANO	
NGFW musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury.	ANO	
NGFW musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů	ANO	
NGFW musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty.	ANO	

VPN:		
NGFW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	ANO	
NGFW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2)	ANO	
Počet současně připojených uživatelů nesmí být licenčně omezený	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z mobilních operačních systémů Android a iOS	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z klientských a serverových operačních systémů Linux	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení bez použití klienta pomocí webového portálu	ANO	
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	
Dodávané řešení musí umožnit přizpůsobení notifikace koncového uživatele o vypršení relace, aby se předešlo nechtěnému odhlášení.	ANO	
Propustnost IPSec musí být alespoň 4 Gb/s	ANO	4.1Gbps

Správa řešení:		
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru.	ANO	
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management serveru.	ANO	
Připojení ke GUI musí podporovat šifrování TLSv1.3	ANO	
GUI musí obsahovat offline kontextovou nápovědu.	ANO	
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 musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.	ANO	
Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku.	ANO	

NGFW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	ANO	
NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	
NGFW musí podporovat nativní nástroj pro odchycení provozu	ANO	
NGFW musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)	ANO	
NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí NGFW	ANO	
NGFW s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz.	ANO	

Aplikační kontrola:		
NGFW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	ANO	
NGFW musí podporovat identifikaci aplikací na nestandardních portech	ANO	
Identifikace aplikace musí probíhat přímo v NGFW	ANO	
NGFW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	ANO	
NGFW musí podporovat řízení neznámého provozu	ANO	
NGFW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	

Kontrola na úrovni uživatelských identit:		
NGFW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	

NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	
NGFW 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	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulár - Captive Portal	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček	ANO	
NGFW 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	

Dešifrování:		
NGFW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	
NGFW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	
NGFW musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace	ANO	
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	
NGFW musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	
NGFW musí podporovat dešifrování protokolu TLS verze 1.3	ANO	

NGFW musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následne přepošle čistě přefiltrované data zpět do NGFW. (tzv. decryption broker)	ANO	
NGFW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.	ANO	
NGFW musí podporovat OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy	ANO	

Ochrana proti DoS:		
NGFW 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	

QoS:		
NGFW 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	
NGFW musí podporovat prioritizaci provozu na základě DSCP	ANO	
NGFW musí podporovat prioritizaci provozu na základě Identifikované aplikace	ANO	

Logování a reportování:		
NGFW musí obsahovat lokální úložiště logů	ANO	
NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	
NGFW 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	
NGFW musí podporovat přeposílání logů na zařízení třetích stran	ANO	
NGFW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	
Přeposílané logy z NGFW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	ANO	
NGFW musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní NGFW	ANO	

Servisní podpora a licenční plán:		
NGFW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	
Požadovaná délka podpory a platnosti licencí je 5 let od nasazení zařízení do sítě objednatele.	ANO	

Centrální management:		

Řešení musí obsahovat virtuální platformu pro centrální správu všech dodaných firewallů do VMware ESXi, MS Hyper-V prostředí	ANO	
Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat všechny dodané HW appliance včetně všech virtuálních kontextů	ANO	
Centrální management musí podporovat zběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci	ANO	
Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu	ANO	
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní NGFW a zároveň přes grafické rozhraní centrálního managementu	ANO	
Administrátor musí mít možnost importovat NGFW konfiguraci do centrálního managementu	ANO	
Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat se grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami	ANO	
Řešení musí obsahovat podporu statických Security Group Tags pro Cisco TrustSec	ANO	
Administrátor musí mít možnost zapsat změny i při čekajících změnách od ostatních administrátorů.	ANO	
Centrální management musí umět v reálném čase zkontrolovat plánověné změny v konfiguraci při zápisu a zablokovat ty, které neodpovídají předepsaným pravidlům.	ANO	

Sandboxing:		
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.	ANO	
Sandbox systém musí být od stejného výrobce jako je NGFW, ale nemusí být HW součástí NGFW	ANO	
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý;	ANO	
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	ANO	
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C.	ANO	
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	ANO	
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní NGFW	ANO	
Aktualizace zero-day signatur musí být instalována do NGFW v reálnem čase, čili s nulovou prodlevou	ANO	
NGFW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.	ANO	

NGFW musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu.	ANO	
NGFW musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky.	ANO	
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí.	ANO	
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita.	ANO	
Sandbox musí rozpoznat, které závisloti malware potřebuje k tomu, aby se spustil a umí je nasimulovat.	ANO	

Bezpečnostní funkcionality:		
NGFW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	
NGFW 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	
NGFW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW 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	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	
NGFW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	
NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; NGFW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	
NGFW musí podporovat import SNORT signatur	ANO	
NGFW 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	
NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	

NGFW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	
NGFW musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane.	ANO	
NGFW musí umět zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení.	ANO	
NGFW musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	ANO	
NGFW musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase.	ANO	
NGFW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování	ANO	
NGFW musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.	ANO	

URL filtering:		
NGFW musí obsahovat nativní podporu pro využívání databáze URL	ANO	
URL databáze musí být od stejného výrobce jako je NGFW	ANO	
NGFW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	ANO	
NGFW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	ANO	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	
NGFW musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní NGFW bez nutnosti kontaktování technické podpory	ANO	

Výkonný pobočkový firewall

Název zařízení-model:	PAN-PA-455		
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 a pod.. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW	ANO	
	Výrobce NGFW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls v posledním aktuálním reportu společnosti Gartner	ANO	
Požadavky na HW architekturu:			
	NGFW musí být typu HW appliance	ANO	
	Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"	ANO	
	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	
	NGFW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	
	NGFW musí obsahovat minimálně 2 metalických datových rozhraní o rychlosti 1Gb/s a 4 metalických datových rozhraní s funkcí PoE o rychlosti 1Gb/s	ANO	2xSFP,2xRJ45,4xRJ45/PoE
	NGFW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu NGFW	ANO	
	NGFW musí být schopen ukládat logové údaje na interní storage o velikosti minimálně 128 GB	ANO	128 GB eMMC
	NGFW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	
	NGFW musí být rozměrově kompatibilní s 19“ rozvaděčem	ANO	
	NGFW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V	ANO	
Požadavky na High Availability (HA):			
	NGFW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení	ANO	
	NGFW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	ANO	
	NGFW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti i v geograficky oddělených lokalitách	ANO	
	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	

NGFW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy	ANO	

Obecné výkonové parametry:		
Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň 3,1 Gb/s (app mix)	ANO	3.6 Gbps
Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 2 Gb/s (app mix)	ANO	2.3 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 300 000	ANO	300000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 54 000	ANO	56000

Síťová funkcionalita:		
NGFW musí plně podporovat IPv4 i IPv6	ANO	
NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	
NGFW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	
NGFW musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)	ANO	
NGFW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	ANO	
NGFW musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směřování.	ANO	
NGFW musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směřování.	ANO	
NGFW musí podporovat nástroj pro pokročilé směřování (Advanced Routing Engine)	ANO	
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	
NGFW musí podporovat napájení PoE (Power Over Ethernet) na připojená síťová zařízení	ANO	
NGFW musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let	ANO	
NGFW musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury.	ANO	
NGFW musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů	ANO	
NGFW musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty.	ANO	

VPN:		
NGFW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	ANO	
NGFW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2)	ANO	
Počet současně připojených uživatelů nesmí být licenčně omezený	ANO	

NGFW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z mobilních operačních systémů Android a iOS	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z klientských a serverových operačních systémů Linux	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení bez použití klienta pomocí webového portálu	ANO	
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	
Dodávané řešení musí umožnit přizpůsobení notifikace koncového uživatele o vypršení relace, aby se předešlo nechtěnému odhlášení.	ANO	
Propustnost IPSec musí být alespoň 1,5 Gb/s	ANO	1.8Gbps

Správa řešení:		
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru.	ANO	
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management serveru.	ANO	
Připojení ke GUI musí podporovat šifrování TLSv1.3	ANO	
GUI musí obsahovat offline kontextovou nápovědu.	ANO	
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 musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.	ANO	
Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku.	ANO	
NGFW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	ANO	
NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	
NGFW musí podporovat nativní nástroj pro odchycení provozu	ANO	
NGFW musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)	ANO	
NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí NGFW	ANO	

NGFW s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz.	ANO	

Aplikační kontrola:		
NGFW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	ANO	
NGFW musí podporovat identifikaci aplikací na nestandardních portech	ANO	
Identifikace aplikace musí probíhat přímo v NGFW	ANO	
NGFW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	ANO	
NGFW musí podporovat řízení neznámého provozu	ANO	
NGFW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	

Kontrola na úrovni uživatelských identit:		
NGFW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	
NGFW 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	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog	ANO	

NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulár - Captive Portal	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček	ANO	
NGFW 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	

Dešifrování:		
NGFW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	
NGFW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	
NGFW musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace	ANO	
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	
NGFW musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	
NGFW musí podporovat dešifrování protokolu TLS verze 1.3	ANO	
NGFW musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následne přepošle čistě přefiltrované data zpět do NGFW. (tzv. decryption broker)	ANO	
NGFW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.	ANO	
NGFW musí podporovat OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy	ANO	

Ochrana proti DoS:		
NGFW 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	

QoS:

NGFW 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	
NGFW musí podporovat prioritizaci provozu na základě DSCP	ANO	
NGFW musí podporovat prioritizaci provozu na základě Identifikované aplikace	ANO	

Logování a reportování:		
NGFW musí obsahovat lokální úložiště logů	ANO	
NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	
NGFW 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	
NGFW musí podporovat přeposílání logů na zařízení třetích stran	ANO	
NGFW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	
Přeposílané logy z NGFW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	ANO	
NGFW musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní NGFW	ANO	

Servisní podpora a licenční plán:		
NGFW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	
Požadovaná délka podpory a platnosti licencí je 5 let od nasazení zařízení do sítě objednatele.	ANO	

Centrální management:		
Řešení musí obsahovat virtuální platformu pro centrální správu všech dodaných firewallů do VMware ESXi prostředí	ANO	
Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat všechny dodané HW appliance včetně všech virtuálních kontextů	ANO	
Centrální management musí podporovat zběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci	ANO	
Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu	ANO	
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní NGFW a zároveň přes grafické rozhraní centrálního managementu	ANO	
Administrátor musí mít možnost importovat NGFW konfiguraci do centrálního managementu	ANO	

Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat se grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami	ANO	
Řešení musí obsahovat podporu statických Security Group Tags pro Cisco TrustSec	ANO	
Administrátor musí mít možnost zapsat změny i při čekajících změnách od ostatních administrátorů.	ANO	
Centrální management musí umět v reálném čase zkontrolovat plánověné změny v konfiguraci při zápisu a zablokovat ty, které neodpovídají předepsaným pravidlům.	ANO	

Sandboxing:		
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.	ANO	
Sandbox systém musí být od stejného výrobce jako je NGFW, ale nemusí být HW součástí NGFW	ANO	
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý;	ANO	
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	ANO	
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C.	ANO	
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	ANO	
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní NGFW	ANO	
Aktualizace zero-day signatur musí být instalována do NGFW v reálnem čase, čili s nulovou prodlevou	ANO	
NGFW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.	ANO	
NGFW musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu.	ANO	
NGFW musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky.	ANO	
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí.	ANO	
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita.	ANO	
Sandbox musí rozpoznat, které závisloti malware potřebuje k tomu, aby se spustil a umí je nasimulovat.	ANO	

Bezpečnostní funkcionality:

NGFW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	
NGFW 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	
NGFW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW 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	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	
NGFW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	
NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; NGFW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	
NGFW musí podporovat import SNORT signatur	ANO	
NGFW 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	
NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	
NGFW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	
NGFW musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnejší analýzu a zároveň se stanice na původní malware stránku nedostane.	ANO	
NGFW musí umět zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení.	ANO	
NGFW musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	ANO	

NGFW musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase.	ANO	
NGFW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování	ANO	
NGFW musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.	ANO	

URL filtering:		
NGFW musí obsahovat nativní podporu pro využívání databáze URL	ANO	
URL databáze musí být od stejného výrobce jako je NGFW	ANO	
NGFW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	ANO	
NGFW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	ANO	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	
NGFW musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní NGFW bez nutnosti kontaktování technické podpory	ANO	

Standardní pobočkový firewall	
Název zařízení-model:	**PAN-PA-415**
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 a pod.. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW	ANO	
Výrobce NGFW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls v posledním aktuálním reportu společnosti Gartner	ANO	

Požadavky na HW architekturu:		
NGFW musí být typu HW appliance	ANO	
Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"	ANO	
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	
NGFW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	
NGFW musí obsahovat minimálně 2 metalických datových rozhraní o rychlosti 1Gb/s a 4 metalických datových rozhraní s funkcí PoE o rychlosti 1Gb/s	ANO	1xSFP,4xRJ45, 4xRJ45/PoE
NGFW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu NGFW	ANO	
NGFW musí být schopen ukládat logové údaje na interní storage o velikosti minimálně 128 GB	ANO	128GB eMMC
NGFW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	
NGFW musí být rozměrově kompatibilní s 19“ rozvaděčem	ANO	
NGFW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V	ANO	

Požadavky na High Availability (HA):		
NGFW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení	ANO	
NGFW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	ANO	
NGFW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti i v geograficky oddělených lokalitách	ANO	
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	
NGFW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy	ANO	

Obecné výkonové parametry:

Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň 1,3 Gb/s (app mix)	ANO	1.5Gbps
Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 0,6 Gb/s (app mix)	ANO	0.8Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 60 000	ANO	64000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 10 000	ANO	11400

Síťová funkcionalita:		
NGFW musí plně podporovat IPv4 i IPv6	ANO	
NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	
NGFW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	
NGFW musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port)	ANO	
NGFW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	ANO	
NGFW musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směřování.	ANO	
NGFW musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směřování.	ANO	
NGFW musí podporovat nástroj pro pokročilé směřování (Advanced Routing Engine)	ANO	
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	
NGFW musí podporovat napájení PoE (Power Over Ethernet) na připojená síťová zařízení	ANO	
NGFW musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let	ANO	
NGFW musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury.	ANO	
NGFW musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů	ANO	
NGFW musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty.	ANO	

VPN:		
NGFW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	ANO	
NGFW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2)	ANO	
Počet současně připojených uživatelů nesmí být licenčně omezený	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení z mobilních operačních systémů Android a iOS	ANO	

NGFW musí pro Remote Access VPN poskytovat připojení z klientských a serverových operačních systémů Linux	ANO	
NGFW musí pro Remote Access VPN poskytovat připojení bez použití klienta pomocí webového portálu	ANO	
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	
Dodávané řešení musí umožnit přizpůsobení notifikace koncového uživatele o vypršení relace, aby se předešlo nechtěnému odhlášení.	ANO	
Propustnost IPSec musí být alespoň 0,6 Gb/s	ANO	0.65Gbps

Správa řešení:		
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru.	ANO	
GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management serveru.	ANO	
Připojení ke GUI musí podporovat šifrování TLSv1.3	ANO	
GUI musí obsahovat offline kontextovou nápovědu.	ANO	
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 musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.	ANO	
Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku.	ANO	
NGFW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	ANO	
NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	
NGFW musí podporovat nativní nástroj pro odchycení provozu	ANO	
NGFW musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)	ANO	
NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí NGFW	ANO	
NGFW s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz.	ANO	

Aplikační kontrola:		
NGFW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	ANO	
NGFW musí podporovat identifikaci aplikací na nestandardních portech	ANO	
Identifikace aplikace musí probíhat přímo v NGFW	ANO	
NGFW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	ANO	
NGFW musí podporovat řízení neznámého provozu	ANO	
NGFW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	

Kontrola na úrovni uživatelských identit:		
NGFW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	
NGFW musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	
NGFW 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	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	

NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulár - Captive Portal	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)	ANO	
NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček	ANO	
NGFW 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	

Dešifrování:		
NGFW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	
NGFW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	
NGFW musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace	ANO	
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	
NGFW musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	
NGFW musí podporovat dešifrování protokolu TLS verze 1.3	ANO	
NGFW musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následne přepošle čistě přefiltrované data zpět do NGFW. (tzv. decryption broker)	ANO	
NGFW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.	ANO	
NGFW musí podporovat OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy	ANO	

Ochrana proti DoS:		
NGFW 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	

QoS:		
NGFW 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	
NGFW musí podporovat prioritizaci provozu na základě DSCP	ANO	

NGFW musí podporovat prioritizaci provozu na základě Identifikované aplikace	ANO	

Logování a reportování:		
NGFW musí obsahovat lokální úložiště logů	ANO	
NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	
NGFW 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	
NGFW musí podporovat přeposílání logů na zařízení třetích stran	ANO	
NGFW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	
Přeposílané logy z NGFW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	ANO	
NGFW musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní NGFW	ANO	

Servisní podpora a licenční plán:		
NGFW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	
Požadovaná délka podpory a platnosti licencí je 5 let od nasazení zařízení do sítě objednatele.	ANO	

Centrální management:		
Řešení musí obsahovat virtuální platformu pro centrální správu všech dodaných firewallů do VMware ESXi prostředí	ANO	
Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat všechny dodané HW appliance včetně všech virtuálních kontextů	ANO	
Centrální management musí podporovat zběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci	ANO	
Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu	ANO	
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní NGFW a zároveň přes grafické rozhraní centrálního managementu	ANO	
Administrátor musí mít možnost importovat NGFW konfiguraci do centrálního managementu	ANO	
Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat se grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami	ANO	
Řešení musí obsahovat podporu statických Security Group Tags pro Cisco TrustSec	ANO	

Administrátor musí mít možnost zapsat změny i při čekajících změnách od ostatních administrátorů.	ANO	
Centrální management musí umět v reálném čase zkontrolovat plánověné změny v konfiguraci při zápisu a zablokovat ty, které neodpovídají předepsaným pravidlům.	ANO	

Sandboxing:		
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.	ANO	
Sandbox systém musí být od stejného výrobce jako je NGFW, ale nemusí být HW součástí NGFW	ANO	
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý;	ANO	
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	ANO	
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C.	ANO	
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	ANO	
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní NGFW	ANO	
Aktualizace zero-day signatur musí být instalována do NGFW v reálnem čase, čili s nulovou prodlevou	ANO	
NGFW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.	ANO	
NGFW musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu.	ANO	
NGFW musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky.	ANO	
Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí.	ANO	
Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita.	ANO	
Sandbox musí rozpoznat, které závisloti malware potřebuje k tomu, aby se spustil a umí je nasimulovat.	ANO	

Bezpečnostní funkcionality:		
NGFW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	
NGFW 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	

NGFW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW 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	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	
NGFW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
NGFW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	
NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; NGFW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	
NGFW musí podporovat import SNORT signatur	ANO	
NGFW 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	
NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	
NGFW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	
NGFW musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vratí podvrženou IP adresu pro detailnejší analýzu a zároveň se stanice na původní malware stránku nedostane.	ANO	
NGFW musí umět zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení.	ANO	
NGFW musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	ANO	
NGFW musí umět rozpoznat komunikaci ukrytou v DoH (DNS-over-HTTPS) požadavcích a aplikovat potřebná DNS bezpečnostní pravidla v reálném čase.	ANO	
NGFW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování	ANO	
NGFW musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách.	ANO	

URL filtering:

NGFW musí obsahovat nativní podporu pro využívání databáze URL	ANO	
URL databáze musí být od stejného výrobce jako je NGFW	ANO	
NGFW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	ANO	
NGFW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	ANO	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	
NGFW musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní NGFW bez nutnosti kontaktování technické podpory	ANO	

B/ Specifikace služeb

		Popis služby	Splněno (Ano/Ne)	Doba trvání v měsících
	Záruka NBD On-site na všechna zařízení			
		Součástí jsou veškeré potřebné licence a podpora výrobce (HW i SW) alespoň na dobu 5 let od zahájení implementace (podpora 24x7, bezpečnostní aktualizace, aktualizace softwaru, výměna HW, či vadné komponenty).	ANO	60
	Zvýšená podpora při implementaci - certifikovaným administrátorem daného FW s praxí min 5 let u daného FW			

Zvýšená podpora při řešení následujících úkonů prováděných zadavatelem: Vypracování prováděcí dokumentace dle požadavků – LLD (Low Level Design, spolupráce při vytváření Architektury sítě a implementace) Analýza stávajícího stavu (FW, NAT, VPN, segmentace atd...) Návrh akceptačních testů pro jednotlivé typy testovacího provozu Implementace/Instalace managementu Základní konfigurace FW Převod pravidel ze současného zařízení do dodávaného pomocí migračního nástroje Převedení provozu na nové řešení FW Začátek 1. fáze (testovací provoz) – postmigrační podpora dodavatele Pilotní konfigurace aplikační kontroly FW (L7) Pilotní konfigurace IPS Pilotní konfigurace antivir/antimalware funkcionality Pilotní konfigurace SSL/TLS dekrypce Finální doladění konfigurace firewallu Vyhodnocení pilotního provozu Dokumentace skutečného provedení Finální akceptace **Podpora bude poskytována na vyžádání v pracovních dnech od 9 do 17 hodin. Doba reakce dodavatele a zahájení podpory: max. 2 hodiny od vyžádání.**	ANO	4

Následná standardní podpora - certifikovaným administrátorem daného FW s praxí min 5 let u daného FW		
Dodavatel po dobu platnosti licencí a podpory výrobce poskytne konzultační služby kvalifikovaným expertním specialistou pro řešení případných problémů, které se během provozu vyskytnou. **Podpora bude poskytována na vyžádání v pracovních dnech od 9 do 17 hodin. Doba reakce dodavatele a zahájení podpory: max. 2 hodiny od vyžádání.**	ANO	na dobu neurčitou (min. 56 měsíců)

Zaškolení Administrátorů pro správu FW - certifikovaným školitelem/ školicím centrem daného FW		
Zaškolení proběhne v jednom oboustranně dohodnutém termínu v rozsahu min. 40 hodin, počet přítomných administrátorů zadavatele bude max. 6. Školení proběhne oficiálním certifikovaným způsobem od dodané technologie. Výstupem bude certifikace o absolvování školení.	ANO	jednorázově

C/ Požadavky z hlediska kybernetické bezpečnosti

		Popis služby	Splněno (Ano/Ne)	
	Varování NÚKIB ze dne 17.12.2018			
		Nabídka dodavatele neobsahuje žádný hardware, software a služby, před kterými varuje NÚKIB ve svém Varování ze dne 17.12.2018, které se týká technických a programových prostředků společností Huawei a ZTE vč, jejich dceřiných společností.	ANO	
	Varování NÚKIB ze dne 21.3.2022 a 31.5.2022			
		Nabídka dodavatele neobsahuje žádný hardware, software a služby, před kterými varuje NÚKIB ve svém Varování ze dne 21.3.2022 doplněném dne 31.5.2022, kde varuje před hrozbou v oblasti kybernetické bezpečnosti spočívající v nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci.	ANO	

Příloha č. 3

Produktové listy k předmětu plnění

Sériové číslo (PN)	**Popis zařízení a jeho součástí**
PAN-PA-415	Palo Alto Networks PA-415
PAN-SVC-PREM-415-5YR	PA-415, Premium support, 5 years (60 months) term.
PAN-PWR-CORD-EU	Power cord for Continental Europe with IEC-60320 C13 and CEE 7/7 SCHUKO cord ends,10A, 250V max, 6ft
Odkaz na datasheet:	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series-pan-os-11-0
PAN-PA-1410	Palo Alto Networks PA-1410
PAN-SVC-PREM-1410-5YR	PA-1410, Premium support, 5 years (60 months) term.
PAN-PA-1410-BND-CORESEC-5YR	PA-1410, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 5 years (60 months) term
PAN-PWR-CORD-EU	Power cord for Continental Europe with IEC-60320 C13 and CEE 7/7 SCHUKO cord ends,10A, 250V max, 6ft
Odkaz na datasheet:	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-1400-series-pan-os-11-0
PAN-PA-455	Palo Alto Networks PA-455
PAN-PA-455-BND-CORESEC-5YR	PA-455, Precision AI Network Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security and Advanced SD-WAN), 5 years (60 months) term
PAN-SVC-PREM-455-5YR	PA-455, Premium support, 5 years (60 months) term.
PAN-PWR-CORD-EU	Power cord for Continental Europe with IEC-60320 C13 and CEE 7/7 SCHUKO cord ends,10A, 250V max, 6ft
Odkaz na datasheet:	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-400-series-pan-os-11-0
PAN-SFP-SX	SFP form factor, SX 1Gb optical transceiver, 550m reach on OM2 MMF, duplex LC, IEEE 802.3z 1000BASE-SX compliant

PAN-SFP-PLUS-SR	SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant
PAN-PA-1410-GP-5YR-HA2	PA-1410, GlobalProtect subscription, for one (1) device in an HA pair, 5 years (60 months) term.
PAN-SFP-CG	SFP form factor, 1Gb copper transceiver, 100m over Cat5 RJ-45, IEEE 802.3ab 1000BASE-T compliant
Odkaz na datasheet:	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/key-specs-for-paloalto-interface-transceivers
PAN-PRA-25	Panorama central management software, 25 devices
PAN-SVC-PREM-PRA-25-5YR	Premium support 5 year term, Panorama 25 devices
Odkaz na datasheet:	https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/panorama