MINISTERSTVO KULTURY

MKCRX00L3KMC

Kupní smlouva

Č. j.: MK 72578/2023 OITSS

Níže uvedeného dne, měsíce a roku uzavřeli:

Smluvní strany:

Česká republika - Ministerstvo kultury
se sídlem Maltézské náměstí 1, 118 11 Praha 1
zastoupená:
IČO: 000 23 671
DIČ: CZ00023671
bankovní spojení: ČNB, Praha
číslo účtu: 3424-001/0710
osoba pověřená ve věcech technických:
(dále jen „**Objednatel**“)

a

TAKTIK, a.s.
se sídlem Eberlova 1472/9, 155 00 Praha 5
zast.:
IČO: 285 22 869
DIČ: CZ285 22 869
zapsaný v obchodním rejstříku vedeném MS v Praze, oddíl C, vložka 141789
bankovní spojení: Komerční banka a.s.
číslo účtu: 115-2635940257/0100
(dále jen „**Dodavatel**“)

tuto

Kupní smlouvu:

I. Výklad pojmů

1. Pro účely závazkových vztahů založených touto smlouvou a pro výklad jednotlivých ustanovení této smlouvy budou následující termíny vykládány takto:

„Zboží“	Dodávka materiálů, komponentů, hardwaru, softwaru, technické podpory výrobce, pro řešení firewall nové generace v technické specifikaci dle Přílohy č. 1 této smlouvy, která tvoří její nedílnou součást;
„Místo dodání“	budova na adrese Praha 6, Milady Horákové 139;
„Cena“	cena uvedená v ustanovení čl. V./1. této smlouvy;
„Programové vybavení“	software potřebný pro správné fungování hardwaru a všech dalších komponentů Zboží dle specifikace Zboží uvedené v Příloze č. 1 a využívání všech požadovaných funkcí Zboží;
„Licence“	nevýhradní licence nebo podlicence - právo užití Programového vybavení na období 3 let od momentu předání a převzetí Zboží;
„Technická podpora výrobce“	Technická podpora výrobce je podpora poskytovaná přímo výrobcem dodávaného Zboží formou servicedesku pro úroveň poskytované podpory L3, kdy úroveň III (nebo úroveň 3, zkráceně T3 nebo L3) je nejvyšší úrovní podpory v tříúrovňovém modelu technické podpory, která je zodpovědná za řešení nejobtížnějších nebo pokročilých problémů.
„Předávací protokol“	protokol o předání a převzetí Zboží podle ustanovení čl. IV. této smlouvy;

II. Zboží

1. Na základě této smlouvy se Dodavatel zavazuje dodat na svůj náklad a nebezpečí Objednateli Zboží a Objednatel se zavazuje Zboží převzít a zaplatit níže uvedenou Cenu.

2. Dodavatel je povinen dodat Zboží ve specifikaci, rozsahu a kvalitě (jakosti), jak vyplývá z Přílohy č. 1 této smlouvy při splnění parametrů uvedených v Příloze č. 1.

3. Součástí dodání Zboží podle této smlouvy je poskytnutí Licence Objednateli k užití Programového vybavení, a to jako nevýhradní licence nebo podlicence na dobu 3 let od momentu předání a převzetí Zboží za cenu (licenční poplatek) uvedenou v příloze č. 2 této smlouvy, který je jako jedna z položek součástí Ceny uvedené v čl. V.

4. Součástí dodání Zboží podle této smlouvy je poskytnutí Technické podpory výrobce na dobu 3 let od momentu předání a převzetí Zboží za cenu uvedenou v příloze č. 2 této smlouvy, který je jako jedna z položek součástí Ceny uvedené v čl. V.

5. Kromě specifikace Zboží sjednané touto smlouvou musí Zboží odpovídat běžným standardům a požadavkům na kybernetickou bezpečnost dle zákona č. 181/2014 Sb. a jeho prováděcích předpisů.

III. Doba a místo dodání

1. Dodavatel se zavazuje předat Zboží Objednateli do 45 dnů od zveřejnění této smlouvy v Registru smluv dle zákona č. 340/2015 Sb.

2. Dodavatel bere na vědomí, že všichni jeho pracovníci zúčastnění na dodávce Zboží do Místa dodání se musí při vstupu podrobit identifikaci předložením svého občanského průkazu nebo cestovního pasu.

3. Místem dodání Zboží je budova na adrese Praha 6, Milady Horákové 685/14.

IV. Předání a převzetí Zboží

1. Dodavatel je povinen Zboží dodat do Místa dodání v dohodnutém termínu dodání bez vad, a to v kvalitě a se všemi dokumenty a doklady souvisejícími se Zbožím a umožnit Objednateli jeho prohlídku. Hodinu dodání případně další doplňující náležitosti dohodne Dodavatel s kontaktní osobou Objednatele uvedenou v čl. XII/1 této Smlouvy.

2. Poté, co si Objednatel Zboží prohlédne a zkontroluje úplnost dokumentů a dokladů, podepíše Objednatel Předávací protokol. Pro vyloučení pochybností se uvádí, že Objednatel je oprávněn přizvat k prohlédnutí Zboží a kontrole úplnosti dokumentů a dokladů kteréhokoliv svého zaměstnance, zmocněnce či poradce.

3. Pro vyloučení jakýchkoliv pochybností se uvádí, že Objednatel není povinen převzít Zboží, pokud dle jeho posouzení trpí jakýmikoliv vadami, zejména pokud neodpovídá specifikaci Zboží uvedené v této Smlouvě nebo nesplňuje některý z požadavků na Zboží uvedený v příloze č.1 této Smlouvy

V. Cena

1. Objednatel se zavazuje zaplatit Dodavateli Cenu za dodávku Zboží dle této smlouvy, ve výši 1 891 880 Kč + DPH v sazbě platné k tzv. dni zdanitelného plnění dle zákona o dani z přidané hodnoty v platném znění.

2. Cena Zboží uvedená v čl. V/1. se skládá z jednotlivých položek Ceny uvedených v Příloze č. 2.

VI. Splatnost Ceny

1. Cena za Zboží, která je uvedena v čl. V/1. je Dodavatel oprávněn vyúčtovat Objednateli po dodání Zboží a jeho převzetí Objednatelem podle čl. IV. této smlouvy.

2. Po převzetí Zboží Objednatelem vystaví Dodavatel Objednateli daňový doklad (fakturu), kterou vyúčtuje Cenu za Zboží s tím, že splatnost Ceny za Zboží je splatností takto

vystaveného daňového dokladu (faktury) a splatnost daňového dokladu je 30 dnů od jeho prokazatelného doručení Objednateli.

3. Faktura vystavená dle čl. VI/2. musí obsahovat veškeré nutné náležitosti daňového dokladu a její přílohou musí být podepsaný Předávací protokol, ze kterého musí vyplývat, že Objednatel Zboží převzal. V případě, že by faktura neobsahovala veškeré nutné náležitosti, nebo v případě, že by její obsah byl v rozporu s obecně závaznými právními předpisy nebo touto smlouvou, je Objednatel oprávněn takovouto obdrženou fakturu vrátit zpět Dodavateli a splatnost jí vyúčtované Ceny za Zboží pro takovýto případ začne běžet až od momentu, kdy Objednatel od Dodavatele obdrží opravený nebo doplněný daňový doklad (fakturu), jehož obsah bude v souladu s obecně závaznými právními předpisy a touto smlouvou.

VII. Sankce

1. Pro případ porušení závazku Dodavatele dodat Zboží řádně a včas dle této smlouvy, je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 0,1 % z Ceny Zboží za každý den, ve kterém bude v prodlení s tímto svým závazkem dodat Zboží řádně a včas.

2. Smluvní pokuta, a to ani zaplacená smluvní pokuta, se nezapočítává na případnou náhradu škody s tím, že pokud by v příčinné souvislosti s porušením povinnosti Dodavatele vznikla Objednateli škoda, je Dodavatel povinen zaplatit Objednateli vedle smluvní pokuty i náhradu škody, a to v plném rozsahu. Účastníci této smlouvy vylučují aplikaci ustanovení § 2050 obč. zákoníku.

3. Pro případ, že by se Objednatel dostal do prodlení se zaplacením Ceny Zboží podle této smlouvy, je povinen zaplatit Dodavateli úrok z prodlení ve výši dle obecně závazného právního předpisu.

4. Pro případ porušení závazku zhotovitele podle čl. IX/2. je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 4.500,- Kč za každý jednotlivý případ porušení své povinnosti s tím, že vedle smluvní pokutu je zhotovitel povinen zaplatit objednateli případnou náhradu škody v plném rozsahu. Smluvní pokuta se na náhradu škody nezapočítává.

5. Jakékoli smluvní pokuty nebo úroky z prodlení, na které by vznikl nárok jedné ze smluvních stran dle této smlouvy, jsou splatné ve lhůtě 30 kalendářních dnů od momentu jejich písemného vyúčtování druhé straně. Písemným vyúčtováním se rozumí pro účely této smlouvy doručení písemného vyúčtování obsahujícího výzvu k zaplacení.

VIII. Obchodní tajemství a mlčenlivost

1. Dodavatel bere na vědomí, že veškeré informace, ke kterým získá v rámci dodávky Zboží přístup, tvoří součást obchodního tajemství Objednatele a Dodavatel není oprávněn tyto informace bez předchozího písemného souhlasu Objednatele poskytnout jakékoli třetí

osobě, ani je využít ve svůj vlastní prospěch. Zároveň je Dodavatel povinen o této skutečnosti poučit výslovně veškeré své zaměstnance a pracovníky, kteří se budou podílet na dodání Zboží podle této smlouvy a zavázat je ve stejném rozsahu k povinnosti mlčenlivosti.

2. Pro případ porušení jakéhokoli závazku Dodavatele dle čl. VIII/1. je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 500.000,- Kč s tím, že nárok na případnou náhradu škody tímto není dotčen a vedle smluvní pokuty je povinen Dodavatel zaplatit Objednateli i náhradu škody, a to v plném rozsahu.

IX. Záruka za jakost

1. Dodavatel poskytuje Objednateli záruku za jakost Zboží v délce 3 let (dále jen „Záruční doba“). Záruční doba počíná běžet dne následujícího po okamžiku převzetí Zboží.

2. Veškeré vady Zboží je Dodavatel povinen odstranit do 48 hodin po jejich nahlášení (reklamaci) na e-mail uvedený v ustanovení čl. XII. této smlouvy.

3. Účastníci této smlouvy dohodou vylučují použití ustanovení § 1925 obč. zákoníku.

X. Přechod vlastnického práva

1. Vlastnické právo k veškerým součástem Zboží přechází z Dodavatele na Objednatele momentem dodání Zboží do místa dodání Zboží dle ustanovení čl. IV. této smlouvy.

XI. Přechod nebezpečí škody

1. Nebezpečí škody na Zboží a veškerých jeho součástí přechází z Dodavatele na Objednatele momentem předání a převzetí Zboží dle ustanovení čl. IV. této smlouvy.

XII. Kontakty

1. Za Objednatele je ve věcech této smlouvy oprávněn jednat: 


2. Za Dodavatele je ve věcech této smlouvy oprávněn jednat: 
e-mail: 

XIII. Trvání smlouvy

1. Tato Smlouva končí svoji platnost a účinnost:

    a. písemnou dohodou stran, nebo
    b. odstoupením dle této Smlouvy dle čl. XIII/2.

2. Kterákoli ze stran je oprávněna od Smlouvy odstoupit, pokud druhá strana poruší své smluvní povinnosti podstatným způsobem. Podstatným porušením se rozumí:

    a. Zboží nesplňuje některý z požadavků dle čl. II této Smlouvy a Dodavatel nezjedná nápravu nebo
    b. Dodavatel nedodá Objednateli Zboží ani v dodatečné lhůtě 45 dnů nad lhůtou definovanou v čl. III nebo
    c. Dodavatel neodstraní vytčenou vadu ani v dodatečné lhůtě 5 pracovních dnů od posledního dne pro odstranění vady dle čl. IX. nebo
    d. Objednatel bude v prodlení s úhradou Ceny delším než 60 dnů od data splatnosti.

3. Projev vůle odstoupit od Smlouvy musí být učiněn písemně a doručen druhé straně. Účinky odstoupení nastávají okamžikem doručení odstoupení druhé straně.

XIV. Postoupení

1. S odkazem na ustanovení § 1895 obč. zákoníku není Dodavatel bez předchozího písemného souhlasu Objednatele oprávněn převést jako postupitel svá práva a povinnosti z této smlouvy nebo z její části třetí osobě, a to ani v případě, že by z této smlouvy ještě nebylo plněno.

2. Dodavatel není oprávněn jako postupitel postoupit na třetí osobu bez předchozího písemného souhlasu Objednatele jakoukoli svoji pohledávku, kterou má nebo bude mít za Objednatelem podle této smlouvy.

XV. Závěrečná ustanovení

1. Tato smlouva může být měněna pouze písemně číslovanými dodatky.

2. Tato Smlouva je platná dnem připojení platného elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, do této Smlouvy a všech jejích jednotlivých příloh, nejsou-li součástí jediného elektronického dokumentu (tj. všech samostatných souborů tvořících v souhrnu Smlouvu), oběma Smluvními stranami.

3. Tato smlouva nabývá účinnosti zveřejněním v Registru smluv dle ustanovení § 6 zákona č. 340/2015 Sb. Zveřejnění v Registru smluv zajistí Objednatel.

XVI. Přílohy

Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1 Technická specifikace Zboží

Příloha č. 2 Struktura Ceny

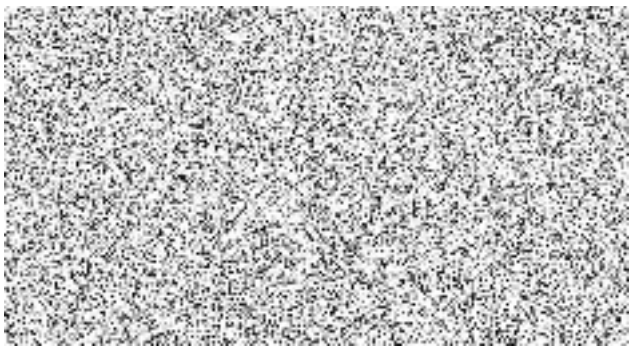
Za objednatele:

V Praze dne (dle doložky el. podpisu)

.....

Za poskytovatele:

V Praze dne (dle doložky el. podpisu)



Příloha č. 1 Technická specifikace Zboží

Vize a cíle zadavatele, popis současného stavu a technické požadavky
Ministerstvo kultury vypisuje zakázku na obnovu a doplnění systému pro filtrování příchozí a odchozí elektronické komunikace (Firewall nové generace – NGFW) dle požadavků uvedených dále. V současné době Ministerstvo kultury používá kromě NGFW jež jsou předmětem obměny v rámci této zakázky ještě další bezpečnostní technologie společnosti Palo Alto Networks a z důvodu kompatibility s řešením pro centrální správu firewallů, konfigurací pravidel a ostatních napojených provozovaných systémů je požadováno zachování stejného výrobce řešení NGFW a to z důvodu technologické kompatibility, servisní kontinuity (soutěžené kompetence dodavatele SLA) a zejména zajištění bezpečnostní funkčnosti celkového řešení. Cluster i pobočkový NGFW budou integrovány do stávajícího bezpečnostního řešení a napojeny na správu a log management. Předmětem obnovy a rozšíření je obnova dvojice centrálních firewallů a dvou pobočkových firewallů. Dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 roky pro všechny požadované bezpečnostní a síťové funkce. V případě, že dosažení požadované výkonnosti vyžaduje doplnit řešení o jakýkoliv typ HW akceleračního modulu, tak tento modul musí být součástí dodávky. Součástí dodávky také musí být přímá technická podpora výrobce (zadavatel musí mít přímý kontakt na centrum technické podpory výrobce) na stejnou dobu, a to v režimu 24x7. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
Cluster NGFW (Next Generation FireWall) perimetru Požadujeme firewall typu NGFW zapojený v režimu vysoké dostupnosti, dle níže uvedené specifikace. Stávající řešení je složeno z dvojice firewallů Palo Alto Networks včetně aktivních předplatných. Firewall řešení je využito jako hlavní síťový perimetr a zároveň pro segmentaci vnitřní sítě (interní segmentační firewall). Z toho důvodu klademe vysoké požadavky na výkonnost a možnosti práce s virtuálními kontexty. Předmětem této zakázky je výměna HW NGFW tohoto clusteru v režimu 1:1. **Pobočkový NGFW** Na pobočkách MKČR je v současnosti nasazen NGFW Palo Alto Networks a je požadována jeho výměna. Nový NGFW bude sloužit primárně ke kontrole a směrování síťového provozu přes NGFW cluster umístěný v centrálním datacentru. Z toho důvodu není vyžadováno pokrytí pobočkových NGFW stejnými předplatnými, jako pro NGFW pro centrální cluster.

Požadavky a jejich splnění			Splněno (ANO / NE)	Popis řešení / poznámka
A				
A	**NGFW Cluster perimetru**			
	A1	**Bezpečnostní zařízení typu firewall nové generace (dále též pouze FW) je jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic apod. Zároveň je tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW. Požadavky na HW architekturu:**		

	1	Všechny parametry propustnosti dodavatel uvede v real world mix paketech, tzv. "application mix".	ANO	požadavek splněn
	2	FW je typu HW appliance a je vyžadována dodávka identických 2ks v HA zapojení	ANO	2x Palo Alto Networks PA-1410
	3	Modul pro zpracování dat je v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění.	ANO	požadavek splněn
	4	Kabeláž potřebná pro HA zapojení v délce 3m je součástí dodávky.	ANO	kabel je součástí dodávky
	5	FW obsahuje jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI.	ANO	požadavek splněn
	6	FW obsahuje alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW.	ANO	požadavek splněn
	7	FW je schopen ukládat logové údaje na interní SSD disk o velikosti minimálně 120 GB	ANO	120 GB
	8	FW podporuje agregaci portů pomocí protokolu 802.3ad (LACP).	ANO	požadavek splněn
	9	FW je rozměrově kompatibilní s 19“ rozvaděčem.	ANO	výška 1U
	10	FW podporuje zdroj napájení AC 230V.	ANO	požadavek splněn
	A2	**Požadavky na počty a typy síťových rozhraní:**		
	1	4x 1 GbE síťových rozhraní typu RJ45 nebo SFP	ANO	8x 10/100/1000 Mbe RJ45
	2	4 x 10 GbE síťových rozhraní typu SFP+	ANO	4x 1/10 Gbe SFP/SFP+
	3	Dedikovaný port 1/10 GbE pro HA	ANO	10 Gbe HA HSCI
	4	FW obsahuje redundantní napájecí zdroj	ANO	požadavek splněn
	A3	**Požadavky na High Availability (HA):**		
	1	FW podporuje režim HA v módu Active-Passive složený alespoň ze dvou zařízení- Pokud tato funkce vyžaduje licenci, tak tato licence musí být součástí dodávky.	ANO	požadavek splněn
	2	V obou typech HA jsou veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes FW.	ANO	požadavek splněn
	3	FW je schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy.	ANO	požadavek splněn
	A4	**Obecné výkonové parametry:**		

	1	Požadované výkonové parametry nabízeného řešení doloží dodavatel oficiálním produktovým listem nebo datasheetem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání zadavatele, pro tyto účely je dodavatel povinen poskytnout i testovací platformu (packet generator). Zadavatel si zároveň vyhrazuje právo na otestování výkonových parametrů, stejně jako vybraných bezpečnostních funkcí.	ANO	datasheet je přílohou nabídky
	2	Počet současně navázaných spojení firewallu min. 900 000	ANO	945 000
	3	Počet nových spojení za sekundu min. 80 000	ANO	100 000
	4	Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 3 Gbps (měřeno na provozu simulujícím reálnou komunikaci/real world traffic).	ANO	3,2 Gbps
	A5	**Síťová funkcionalita:**		
	1	FW plně podporuje IPv4 i IPv6.	ANO	požadavek splněn
	2	FW podporuje zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP.	ANO	požadavek splněn
	3	FW podporuje překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64.	ANO	požadavek splněn
	4	FW podporuje směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding).	ANO	požadavek splněn
	5	PBF je možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	požadavek splněn
	A6	**VPN:**		
	1	FW podporuje site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený.	ANO	požadavek splněn

	2	FW podporuje Remote Access VPN pomocí protokolů IPSec a SSL (TLS, či DTLS). Počet současně připojených uživatelů nesmí být licenčně omezený.	ANO	požadavek splněn
	3	Celková propustnost IPSEC VPN při použití 64KB HTTP transakcí a zapnutým logováním min. 4 Gbps	ANO	4,6 Gbps
	A7	**Management:**		
	1	Jednotlivé HW appliance obsahují plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI podporuje šifrování.	ANO	požadavek splněn
	2	Jednotlivé HW appliance obsahují plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI podporuje šifrování.	ANO	požadavek splněn
	3	Jednotlivé HW appliance umožňují použití šablon pro bootstraping nových FW použitím USB flash disku.	ANO	požadavek splněn
	4	FW pro autentizaci a autorizaci administrátorů podporuje protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát.	ANO	požadavek splněn
	5	FW obsahuje nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu.	ANO	požadavek splněn
	6	FW podporuje nativní nástroj pro odchycení provozu.	ANO	požadavek splněn
	7	FW management podporuje práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.	ANO	požadavek splněn
	8	Správa všech zařízení pracujících v režimu vysoké dostupnosti probíhá jednotně přes společné grafické konfigurační rozhraní.	ANO	požadavek splněn
	9	Grafické konfigurační rozhraní pro správu celého clusteru je dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.	ANO	požadavek splněn
	10	FW cluster podporuje "floating IP"	ANO	požadavek splněn

	A8	**Aplikační kontrola:**		
	1	FW podporuje aplikační detekci a kontrolu jako svou nativní funkcionalitu.	ANO	požadavek splněn
	2	Přiřazení povolené či zakázané aplikace je nativní součástí vytváření standardního bezpečnostního pravidla.	ANO	požadavek splněn
	3	Definovaná aplikace představuje "match kritérium" při policy lookup.	ANO	požadavek splněn
	4	FW podporuje identifikaci aplikací napříč všemi porty/protokoly.	ANO	požadavek splněn
	5	FW podporuje identifikaci a blokaci aplikací na nestandardních portech v rámci jediného pravidla.	ANO	požadavek splněn
	6	Identifikace aplikace probíhá přímo ve FW.	ANO	požadavek splněn
	7	FW detekuje a zabraňuje aplikaci měnit porty, tzv. port-hopping.	ANO	požadavek splněn
	8	FW podporuje řízení neznámého provozu.	ANO	požadavek splněn
	9	FW umožňuje tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO	požadavek splněn
	A9	**Kontrola na úrovni uživatelských identit:**		
	1	FW podporuje vytváření bezpečnostních pravidel na základě uživatelských identit.	ANO	požadavek splněn
	2	Volba uživatelské identity jsou nativní součástí vytváření standardního bezpečnostního pravidla.	ANO	požadavek splněn
	3	Uživatelská identita představuje "match kritérium" při policy lookup.	ANO	požadavek splněn
	4	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení.	ANO	požadavek splněn

	5	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler.	ANO	požadavek splněn
	6	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance.	ANO	požadavek splněn
	7	FW podporuje získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins).	ANO	požadavek splněn
	8	FW podporuje získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta).	ANO	požadavek splněn
	A10	**Dešifrování:**		
	1	FW podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům.	ANO	požadavek splněn
	2	FW podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru.	ANO	požadavek splněn
	3	FW podporuje dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace.	ANO	požadavek splněn
	4	Dešifrovaný provoz je možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita.	ANO	požadavek splněn
	5	FW podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz.	ANO	požadavek splněn
	A11	**Bezpečnostní funkcionality:**		
	1	FW podporuje zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu.	ANO	požadavek splněn
	2	FW umožňuje tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO	požadavek splněn

	3	FW obsahuje integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla.	ANO	požadavek splněn
	4	Antivirus je schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB.	ANO	požadavek splněn
	5	FW umožňuje tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO	požadavek splněn
	6	FW podporuje možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci.	ANO	požadavek splněn
	7	FW podporuje v bezpečnostních pravidlech použití externích dynamických seznamů.	ANO	požadavek splněn
	8	FW poskytuje možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu.	ANO	požadavek splněn
	9	FW podporuje analýzu DNS dotazu tzv. Sinkhole funkcí, která na dotaz malware DNS URL vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane.	ANO	požadavek splněn
	10	FW poskytuje možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	ANO	požadavek splněn
	11	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet definice pro vlastní aplikace.	ANO	požadavek splněn
	12	Funkce rozpoznání populárních internetových aplikací založená na výrobcem udržované a aktualizované databázi veřejných IP adres, na kterých jsou zkoumané služby hostovány; možnost použití informací z této databáze jako pro odchozí provoz (uživatelé -> internetové služby) tak i pro příchozí provoz (např. za účelem blokování komunikace z Tor exit nódů).	ANO	požadavek splněn

	13	Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze. Požadujeme vynikající pokrytí českých internetových domén.	ANO	požadavek splněn
	14	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů.	ANO	požadavek splněn
	15	Funkce filtrace přenášených souborů umožňující definovat politiku na přenos souborů přes protokoly (CIFS/SMB, FTP/s, http/s, imap/s, pop3/s, smtp/s) v odchozím a příchozím směru podle vnitřní struktury (typu) souboru nebo koncovky.	ANO	požadavek splněn
	16	Funkce ochrany před únikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet. Možnost definovat citlivá data minimálně na principu tzv. watermark a také definicí regulárním výrazem.	ANO	požadavek splněn
	17	Funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně na základě administrátorem definovaných adres a také podpora TLS 1.3 z pohledu inspekce sítového provozu SSL kontrolou ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On.	ANO	požadavek splněn
	18	Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky.	ANO	požadavek splněn
	19	Funkce klientské VPN (přístup do vpn v tunelovém režimu s vpn klientem; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů; ssl vpn nebo ipsec vpn).	ANO	požadavek splněn
	20	Site-to-site ipsec vpn s podporou statického i dynamického routování.	ANO	požadavek splněn
	21	Podpora funkce loadbalancingu s funkcí ssl offload a možností výběru LB metody (min. round robin, IP hash, IP modulo, výběr dle nejmenšího počtu aktivních spojení)	ANO	požadavek splněn

	22	Podpora automatické reakce NGFW na detekovaný incident v síti minimálně pomocí: automatické karantény problematických klientů, notifikace administrátora.	ANO	požadavek splněn
	23	Podpora dvoufaktorového ověřování uživatelů a administrátorů pomocí technicky OTP (mobilní OTP aplikace či hw OTP token). Tato funkce může být podporována jako samostatné řešení, funkčně integrované s firewallem, nebo jako nativní součást firewallu.	ANO	požadavek splněn
	A12	**Ochrana proti DoS:**		
	1	FW obsahuje nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a aplikace.	ANO	požadavek splněn
	A13	**QoS:**		
	1	FW poskytuje možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.).	ANO	požadavek splněn
	2	FW podporuje prioritizaci provozu na základě DSCP.	ANO	požadavek splněn
	3	FW podporuje prioritizaci provozu na základě Identifikované aplikace.	ANO	požadavek splněn
	A14	**URL filtering:**		
	1	FW obsahuje nativní podporu pro využívání databáze URL.	ANO	požadavek splněn
	2	URL databáze je od stejného výrobce jako je FW.	ANO	požadavek splněn
	3	FW je schopen použít URL kategorii v definici bezpečnostního pravidla.	ANO	požadavek splněn
	4	FW podporuje vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele.	ANO	požadavek splněn

	5	URL databáze je dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra.	ANO	požadavek splněn
	6	FW umožňuje požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní FW bez nutnosti kontaktování technické podpory.	ANO	požadavek splněn
	A15	**Servisní podpora a licenční plán:**		
	1	FW podporuje licenční model nezávislý na počtu ochraňovaných koncových systémů.	ANO	požadavek splněn
	2	Součástí NGFW jsou licence v délce trvání 3 let zajišťující minimálně následující plnou funkcionalitu: -Ochrana před škodlivým kódem (threat prevention) -Pokročilá ochrana před škodlivými URL založená na detekci chování v reálném čase -Ochrana před neznámými hrozbami (tzv zero-day) -Ochrana před zranitelnostmi využívajícími podvržení DNS	ANO	potřebná předplatná jsou součástí nabídky v délce trvání 3 let: Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, DNS Security, SD-WAN, Global protect
B				
B		**Pobočkový NGFW**		
	B1	**Bezpečnostní zařízení typu firewall nové generace (dále též pouze FW) je jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic apod. Zároveň je tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW.** **Požadavky na HW architekturu:**		
	1	Všechny parametry propustnosti dodavatel uvádí v real world mix paketech, tzv. "application mix".	ANO	požadavek splněn
	2	FW je typu HW appliance – 2 ks pro pobočky MKČR	ANO	2x Palo Alto Networks PA-410
	3	Modul pro zpracování dat je v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění.	ANO	požadavek splněn
	4	FW obsahuje jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI.	ANO	požadavek splněn

	5	FW obsahuje alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW.	ANO	požadavek splněn
	6	FW podporuje agregaci portů pomocí protokolu 802.3ad (LACP).	ANO	požadavek splněn
	B2	**Požadavky na počty a typy síťových rozhraní:**		
	1	6x 1 GbE síťových rozhraní typu RJ45	ANO	7x 1 Gbe RJ45
	B3	**Obecné výkonové parametry:**		
	1	Požadované výkonové parametry nabízeného řešení doloží dodavatel oficiálním produktovým listem nebo datasheetem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání zadavatele, pro tyto účely je dodavatel povinen poskytnout i testovací platformu (packet generator). Zadavatel si zároveň vyhrazuje právo na otestování výkonových parametrů, stejně jako vybraných bezpečnostních funkcí.	ANO	Datasheet je součástí nabídky
	2	Počet současně navázaných spojení firewallu min. 60 000	ANO	64 000
	3	Počet nových spojení za sekundu min. 10 000	ANO	11 000
	4	Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV dosahuje hodnoty alespoň 600 Mb/s (app mix)	ANO	600 Mb/s
	B4	**Síťová funkcionalita:**		
	1	FW plně podporuje IPv4 i IPv6.	ANO	požadavek splněn
	2	FW podporuje zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP.	ANO	požadavek splněn
	3	FW podporuje překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64.	ANO	požadavek splněn
	4	FW podporuje směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding).	ANO	požadavek splněn
	5	PBF je možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	požadavek splněn
	B5	**VPN:**		
	1	FW podporuje site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený.	ANO	požadavek splněn

	2	FW podporuje Remote Access VPN pomocí protokolů IPSec a SSL (TLS, či DTLS). Počet současně připojených uživatelů nesmí být licenčně omezený.	ANO	požadavek splněn
	3	Celková propustnost IPSEC VPN při použití 64 KB HTTP transakcí a zapnutým logování min. 800 Mbps.	ANO	920 Mbps
	B6	**Management:**		
	1	Jednotlivé HW appliance obsahují plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI podporuje šifrování.	ANO	požadavek splněn
	2	Jednotlivé HW appliance obsahují plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI podporuje šifrování.	ANO	požadavek splněn
	3	Jednotlivé HW appliance umožňují použití šablon pro bootstraping nových FW použitím USB flash disku.	ANO	požadavek splněn
	4	FW pro autentizaci a autorizaci administrátorů podporuje protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát.	ANO	požadavek splněn
	5	FW obsahuje nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu.	ANO	požadavek splněn
	6	FW podporuje nativní nástroj pro odchycení provozu.	ANO	požadavek splněn
	7	FW management podporuje práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.	ANO	požadavek splněn
	8	Správa všech zařízení pracujících v režimu vysoké dostupnosti probíhá jednotně přes společné grafické konfigurační rozhraní.	ANO	požadavek splněn
	9	Grafické rozhraní je identické, jako v případě centrálního NGFW firewallu.	ANO	požadavek splněn
	10	Grafické konfigurační rozhraní pro správu celého clusteru je dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.	ANO	požadavek splněn
	B7	**Aplikační kontrola:**		

	1	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet definice pro vlastní aplikace.	ANO	požadavek splněn
	2	FW podporuje aplikační detekci a kontrolu jako svou nativní funkcionalitu.	ANO	požadavek splněn
	3	Přiřazení povolené či zakázané aplikace je nativní součástí vytváření standardního bezpečnostního pravidla.	ANO	požadavek splněn
	4	Definovaná aplikace představuje "match kritérium" při policy lookup.	ANO	požadavek splněn
	5	FW podporuje identifikaci aplikací napříč všemi porty/protokoly.	ANO	požadavek splněn
	6	FW podporuje identifikaci aplikací na nestandardních portech.	ANO	požadavek splněn
	7	Identifikace aplikace probíhá přímo ve FW.	ANO	požadavek splněn
	8	FW detekuje a zabraňuje aplikaci měnit porty, tzv. port-hopping.	ANO	požadavek splněn
	9	FW podporuje řízení neznámého provozu.	ANO	požadavek splněn
	10	FW umožňuje tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO	požadavek splněn
	B8	**Kontrola na úrovni uživatelských identit:**		
	1	FW podporuje vytváření bezpečnostních pravidel na základě uživatelských identit.	ANO	požadavek splněn
	2	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On.	ANO	požadavek splněn
	3	Uživatelská identita představuje "match kritérium" při policy lookup.	ANO	požadavek splněn
	4	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení.	ANO	požadavek splněn
	5	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler.	ANO	požadavek splněn
	6	FW podporuje získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance.	ANO	požadavek splněn

	7	FW podporuje získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins).	ANO	požadavek splněn
	8	FW podporuje získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta).	ANO	požadavek splněn
	B9	**Dešifrování:**		
	1	FW podporuje dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům.	ANO	požadavek splněn
	2	FW podporuje dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru.	ANO	požadavek splněn
	3	FW podporuje dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace.	ANO	požadavek splněn
	4	Dešifrovaný provoz je možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita.	ANO	požadavek splněn
	5	FW podporuje dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz.	ANO	požadavek splněn
	6	Podpora TLS 1.3 z pohledu inspekce síťového provozu SSL kontrolou.	ANO	požadavek splněn
	B10	**Management:**		
	1	Jednotlivé HW appliance obsahují plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI podporuje šifrování.	ANO	požadavek splněn
	2	Jednotlivé HW appliance obsahují plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI podporuje šifrování.	ANO	požadavek splněn
	3	Jednotlivé HW appliance umožňují použití šablon pro bootstraping nových FW použitím USB flash disku.	ANO	požadavek splněn
	4	FW pro autentizaci a autorizaci administrátorů podporuje protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát.	ANO	požadavek splněn

	5	FW obsahuje nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu.	ANO	požadavek splněn
	6	FW podporuje nativní nástroj pro odchycení provozu.	ANO	požadavek splněn
	7	FW management podporuje práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem.	ANO	požadavek splněn
	8	Správa všech zařízení pracujících v režimu vysoké dostupnosti probíhá jednotně přes společné grafické konfigurační rozhraní.	ANO	požadavek splněn
	9	Grafické rozhraní je identické, jako v případě centrálního NGFW firewallu.	ANO	požadavek splněn
	10	Grafické konfigurační rozhraní pro správu celého clusteru je dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci.	ANO	požadavek splněn
	B11	**Bezpečnostní funkcionality:**		
	1	FW podporuje zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu.	ANO	požadavek splněn
	2	FW umožňuje tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele.	ANO	požadavek splněn
	3	FW obsahuje integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla.	ANO	požadavek splněn
	4	Antivirus je schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB.	ANO	požadavek splněn
	5	FW podporuje možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci.	ANO	požadavek splněn
	6	FW podporuje v bezpečnostních pravidlech použití externích dynamických seznamů.	ANO	požadavek splněn
	7	FW poskytuje možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu.	ANO	požadavek splněn
	8	FW podporuje analýzu DNS dotazu tzv. Sinkhole funkcí, která na dotaz malware DNS URL vratí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane.	ANO	požadavek splněn

	9	FW poskytuje možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	ANO	požadavek splněn
	10	Funkce rozpoznání populárních internetových aplikací založená na výrobcem udržované a aktualizované databázi veřejných IP adres, na kterých jsou zkoumané služby hostovány; možnost použití informací z této databáze jako pro odchozí provoz (uživatelé -> internetové služby) tak i pro příchozí provoz (např. za účelem blokování komunikace z Tor exit nódů).	ANO	požadavek splněn
	11	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů.	ANO	požadavek splněn
	12	Funkce filtrace přenášených souborů umožňující definovat politiku na přenos souborů přes protokoly (CIFS/SMB, FTP/s, http/s, imap/s, pop3/s, smtp/s) v odchozím a příchozím směru podle vnitřní struktury (typu) souboru nebo koncovky.	ANO	požadavek splněn
	13	Funkce ochrany před únikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet. Možnost definovat citlivá data minimálně na principu tzv. watermark a také definicí regulárním výrazem.	ANO	požadavek splněn
	14	Funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky ze SSL inspekce požadujeme minimálně na základě administrátorem definovaných adres a také na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví, atd.)	ANO	požadavek splněn
	15	Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky.	ANO	požadavek splněn
	16	Funkce klientské VPN (přístup do vpn v tunelovém režimu s vpn klientem; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky vpn uživatelů; ssl vpn nebo ipsec vpn).	ANO	požadavek splněn
	17	Site-to-site ipsec vpn s podporou statického i dynamického routování.	ANO	požadavek splněn

	18	Podpora funkce loadbalancingu s funkcí ssl offload a možností výběru LB metody (min. round robin, IP hash, IP modulo, výběr dle nejmenšího počtu aktivních spojení)	ANO	požadavek splněn
	19	Podpora automatické reakce NGFW na detekovaný incident v síti minimálně pomocí: automatické karantény problematických klientů, notifikace administrátora.	ANO	požadavek splněn
	20	Podpora dvoufaktorového ověřování uživatelů a administrátorů pomocí technicky OTP (mobilní OTP aplikace či hw OTP token). Tato funkce může být podporována jako samostatné řešení, funkčně integrované s firewallem, nebo jako nativní součást firewallu.	ANO	požadavek splněn
	B12	**Ochrana proti DoS:**		
	1	FW obsahuje nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a aplikace.	ANO	požadavek splněn
	B13	**QoS:**		
	1	FW poskytuje možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.).	ANO	požadavek splněn
	2	FW podporuje prioritizaci provozu na základě DSCP.	ANO	požadavek splněn
	3	FW podporuje prioritizaci provozu na základě Identifikované aplikace.	ANO	požadavek splněn
	B14	**URL filtering:**		
	1	Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), výrobcem aktualizovaná a udržovaná databáze. Požadujeme vynikající pokrytí českých internetových domén.	ANO	požadavek splněn
	2	FW obsahuje nativní podporu pro využívání databáze URL.	ANO	požadavek splněn

	3	URL databáze je od stejného výrobce jako je FW.	ANO	požadavek splněn
	4	FW je schopen použít URL kategorii v definici bezpečnostního pravidla.	ANO	požadavek splněn
	5	FW podporuje vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele.	ANO	požadavek splněn
	6	URL databáze je dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra.	ANO	požadavek splněn
	7	FW umožňuje požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní FW bez nutnosti kontaktování technické podpory.	ANO	požadavek splněn
	B15	**Servisní podpora a licenční plán:**		
	1	FW podporuje licenční model nezávislý na počtu ochraňovaných koncových systémů.	ANO	požadavek splněn
	2	Součástí NGFW jsou licence v délce trvání 3 let zajišťující minimálně následující plnou funkcionalitu: -Ochrana před škodlivým kódem (threat prevention)	ANO	Licence Advanced Threat Prevention subscription jsou součástí nabídky v délce trvání 3 let

Příloha č. 2 Struktura Ceny

Položka k ocenění	Četnost	Jednotka	Nabídková cena za jednotku (v Kč bez DPH)	Výše DPH k nabídkové ceně za jednotku (v Kč)	Nabídková cena celkem za položku po zohlednění četnosti (v Kč bez DPH)
HW komponenty	1	komplet	523 350,00 Kč	109 903,50 Kč	523 350,00 Kč
Licence	1	komplet	1 075 540,00 Kč	225 863,40 Kč	1 075 540,00 Kč
Podpora	1	komplet	292 990,00 Kč	61 527,90 Kč	292 990,00 Kč
Celková nabídková cena (v Kč bez DPH)					**1 891 880,00 Kč**
Výše DPH (celkové nabídkové ceny; v Kč)					397 294,80 Kč
Celková nabídková cena (v Kč s DPH)					2 289 174,80 Kč