Smlouva o dílo

uzavřená dle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, níže uvedeného dne, měsíce a roku, mezi:

AUTOCONT a.s.

Sídlo: Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava

IČ: 04308697

DIČ: CZ04308697

Zastoupena: Jindřich Zimola, ředitel regionálního obchodního centra, zmocněný na základě plné moci ze dne 3. 12. 2020

Číslo smlouvy Zhotovitele: RCS-210065

na straně jedné (dále jen jako „zhotovitel“)

a

Vojenská nemocnice Olomouc

Sídlo: Sušilovo nám. 1/5, Klášterní Hradisko, 779 00 Olomouc

IČ: 608 00 691

Zastoupena: plk. gšt. v. z. MUDr. Martin Svoboda, ředitel

na straně druhé (dále jen jako „objednatel“)

(dále zhotovitel a objednatel jen jako „smluvní strany“)

I.
Úvodní prohlášení

Smluvní strany prohlašují a činí nesporným, že tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „VN Olomouc – Ochrana prvků vnitřní sítě“.

(dále jen jako „veřejná zakázka“)

II.
Dílo

Smluvní strany prohlašují a činí nesporným, že na základě této smlouvy se zhotovitel zavazuje provést pro objednatele na svůj náklad a nebezpečí dílo představující:

- dodávku dvou fyzických firewallů v HA režimu a ochran elektronické pošty, publikovaných webových aplikací, surfování, koncových stanic, serverů a zařízení pro vyhodnocování a analýzu logů těchto ochran;
- dodávku prací, tj. implementace do technologického prostředí objednatele (instalace, konfigurace, převod konfigurace stávajících ochranných prvků na nové a převod provozu),

a to v souladu se zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, a objednatel se zavazuje řádně a včas provedené dílo převzít a zaplatit za něj zhotoviteli cenu.

(dále jen jako „dílo“)

III.
Cena díla a platební podmínky

Smluvní strany prohlašují a činí nesporným, že:

a) celková cena díla činí **3 480 000,00 Kč bez DPH**
(slovy: třimilionyčtyřistaosmdesáttisíc korun českých) a je nejvýše přípustná (nepřekročitelná) a platná a účinná po celou dobu provádění díla na základě této smlouvy, která zahrnuje mj. dodávku hardwaru a softwaru a dodávku prací včetně servisní podpory výrobce po dobu pěti let od protokolárního předání díla bez vad a nedodělků;

b) součástí ceny díla jsou tak i veškeré další související vynaložené náklady (např. náklady na dopravu) neuvedené v písm. a) tohoto čl. smlouvy nezbytné k řádnému a včasnému provedení díla s tím, že zhotovitel je oprávněn navýšit cenu díla o příslušnou sazbu DPH či jinou daň v souladu s platnými právními předpisy.

Objednatel prohlašuje a činí nesporným, že je povinen zaplatit zhotoviteli cenu díla na základě faktury – daňového dokladu, jejíž přílohou bude i předávací protokol ve smyslu čl. IV. písm. c) anebo d) této smlouvy, kterou je zhotovitel povinen vystavit v souladu s příslušnými právními předpisy bezodkladně po provedení díla bez vad a nedodělků, a to bezhotovostním převodem na bankovní účet zhotovitele č. 6563752/0800, se splatností 30 dnů ode dne jejího vystavení.

Smluvní strany dále prohlašují a činí nesporným, že objednatel je oprávněn vrátit zhotoviteli vystavenou fakturu – daňový doklad v případě, že příslušná faktura – daňový doklad nebude mít některou ze zákonných či smluvních náležitostí či příloh s tím, že v takovém případě je zhotovitel povinen vystavit po doručení vrácené faktury – daňového dokladu bez zbytečného odkladu novou fakturu – daňový doklad se všemi zákonnými i smluvními náležitostmi včetně příloh. Od okamžiku doručení nové faktury – daňového dokladu dle předchozí věty počíná objednateli běžet nová doba splatnosti.

IV.
Místo a čas plnění

Smluvní strany prohlašují a činí nesporným, že:

a) zhotovitel je povinen provést na svůj náklad a nebezpečí dílo v sídle objednatele;

b) zhotovitel je povinen provést dílo do 9. 12. 2021 v souladu s harmonogramem prací, který se zhotovitel zavazuje vypracovat a předat objednateli v písemné podobě před započetím provádění díla;

c) o předání a převzetí díla bude sepsán a smluvními stranami podepsán předávací protokol, který musí obsahovat alespoň následující skutečnosti:

- identifikace této smlouvy;
- identifikace smluvních stran;
- místo a datum provedení díla, resp. jeho dokončení a předání;
- prohlášení objednatele, zda dílo přebírá s výhradami nebo bez výhrad;
- případné vady a nedodělky díla a lhůtu pro jejich odstranění;

d) zhotovitel je povinen odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole dle písm. c) tohoto čl. smlouvy;

e) v případě odstranění vad a nedodělků ve smyslu písm. c) a d) tohoto čl. smlouvy, bude o předání a převzetí díla bez vad a nedodělků sepsán a smluvními stranami podepsán předávací protokol.

V.
Ostatní ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) v případě provádění byť jen části díla prostřednictvím poddodavatelů zhotovitele, je zhotovitel odpovědný i za případně vzniklou majetkovou újmu (škodu) objednatele v důsledku porušení smluvních či zákonných povinností daného poddodavatele, jako by

ji způsobil sám, a zhotovitel je tak povinen takto vzniklou majetkovou újmu (škodu) objednateli v plném rozsahu nahradit;

b) zhotovitel je povinen být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), kdy příslušnou pojistku je zhotovitel povinen objednateli předložit bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy;

c) zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním;

d) zhotovitel je povinen archivovat originál této smlouvy včetně jejích případných dodatků a jejích příloh, dále veškeré originály účetních dokladů a dalších dokumentů souvisejících s prováděním díla po dobu minimálně deseti let od protokolárního předání díla objednateli bez vad a nedodělků.

VI.
Záruka za jakost díla

Zhotovitel prohlašuje a činí nesporným, že poskytuje na dílo záruku v délce dvacetičtyřměsíců, která počíná běžet okamžikem předání díla bez vad a nedodělků na základě předávacího protokolu ve smyslu čl. IV. této smlouvy.

Smluvní strany prohlašují a činí nesporným, že:

a) pokud objednatel v záruční době zjistí vadu díla, je povinen ji bezodkladně oznámit (postačí e-mailem) zhotoviteli na e-mailovou adresu: servishw@autocont.cz (dále jen jako „reklamace“) s tím, že zhotovitel je povinen vadu odstranit ve lhůtě patnácti dnů od okamžiku doručení reklamace a nahradit objednateli vzniklou majetkovou újmu (škodu) v plném rozsahu se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) doba od doručení reklamace zhotoviteli do doby odstranění vytýkané vady na základě reklamace se do záruční doby nezapočítává a o tuto dobu se záruční doba prodlužuje.

VII.
Smluvní pokuta

Smluvní strany prohlašují a činí nesporným, že:

a) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. II. této smlouvy, resp. povinnost provést pro objednatele na svůj náklad a nebezpečí dílo v souladu se zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. IV. písm. a), b) anebo d) této smlouvy, resp. povinnost provést na svůj náklad a nebezpečí dílo v sídle objednatele, anebo povinnost provést dílo do 9.12.2021 v souladu s harmonogramem prací, který se zhotovitel zavazuje vypracovat a předat objednateli v písemné podobě před započetím provádění díla, anebo povinnost vypracovat a předat objednateli v písemné podobě před započetím provádění díla harmonogram prací, anebo povinnost odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

c) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. V. písm. b) této smlouvy, resp. povinnost být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), anebo povinnost předložit pojistku objednateli bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané

povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

d) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. V. písm. c) této smlouvy, resp. povinnost zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 1% z celkové ceny díla za každý případ takovéhoto porušení se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

e) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. VI. této smlouvy, resp. povinnost odstranit vadu ve lhůtě patnácti dnů od okamžiku doručení reklamace, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

f) ujednáním o smluvních pokutách ve smyslu písm. a) – e) tohoto článku smlouvy není dotčeno právo objednatele na náhradu majetkové újmy (škody) v plném rozsahu, kdy tímto smluvní strany vylučují ust. § 2050 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

VIII.
Odstoupení od smlouvy

Objednatel je oprávněn odstoupit od této smlouvy do doby provedení díla bez vad a nedodělků v těchto případech:

a) bude zahájeno insolvenční řízení ve věci zhotovitele jako dlužníka;

b) bude zahájeno anebo bude zjištěno jakékoliv exekuční řízení proti zhotoviteli jako povinnému;

c) zhotovitel bude v prodlení s provedením díla bez vad a nedodělků alespoň třicet kalendářních dnů;

d) zhotovitel bude provádět dílo v rozporu se zadávacími podmínkami anebo v rozporu s touto smlouvou, ačkoliv byl na tuto skutečnost ze strany objednatele alespoň jedenkrát upozorněn.

IX.
Převzetí nebezpečí změny okolností

Zhotovitel prohlašuje a činí nesporným, že na sebe převzal nebezpečí změny okolností ve smyslu ust. § 1765 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

X.
Závěrečná ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) tato smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., zákon o registru smluv, v platném znění, kdy povinným subjektem je objednatel, a zavazuje se tak tuto smlouvu uveřejnit v registru smluv nejpozději do třiceti dnů ode dne podpisu této smlouvy oběma smluvními stranami;

b) tato smlouva je sepsána ve dvou vyhotoveních takto:

- 1x zhotovitel;
- 1x objednatel;

c) rozhodným právem pro tento závazkový vztah je právo české (právní řád České republiky);

d) tuto smlouvu je možné změnit pouze písemně, kdy pro účely této smlouvy se za písemnou formu nepovažuje výměna emailových či jiných elektronických zpráv;

e) vylučují přijetí nabídky s dodatkem nebo odchylkou ve smyslu ust. § 1740 zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

f) pokud nebylo v této smlouvě ujednáno jinak, řídí se právní vztahy vzniklé z této smlouvy příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

g) tato smlouva byla sepsána dle jejich vážné, pravé a svobodné vůle, kdy na důkaz toho po jejím přečtení činí vlastnoruční podpisy.

Příloha č. 1: technická specifikace

V Ostrava, dne

Jindřich Zimola

Digitálně podepsal Jindřich Zimola
Datum: 2021.08.23 14:29:35 +02'00'

.....

AUTOCONT a.s.
Jindřich Zimola
ředitel regionálního obchodního centra,
zmocněný na základě plné moci ze dne 3. 12. 2020
(zhotovitel)

V Olomouci, dne

MUDr. Martin Svoboda

Digitálně podepsal MUDr. Martin Svoboda
Datum: 2021.09.07 12:18:23 +02'00'

.....

Vojenská nemocnice Olomouc
plk. gšt. v. z. MUDr. Martin Svoboda
ředitel
(objednatel)

Příloha č. 1: technická specifikace

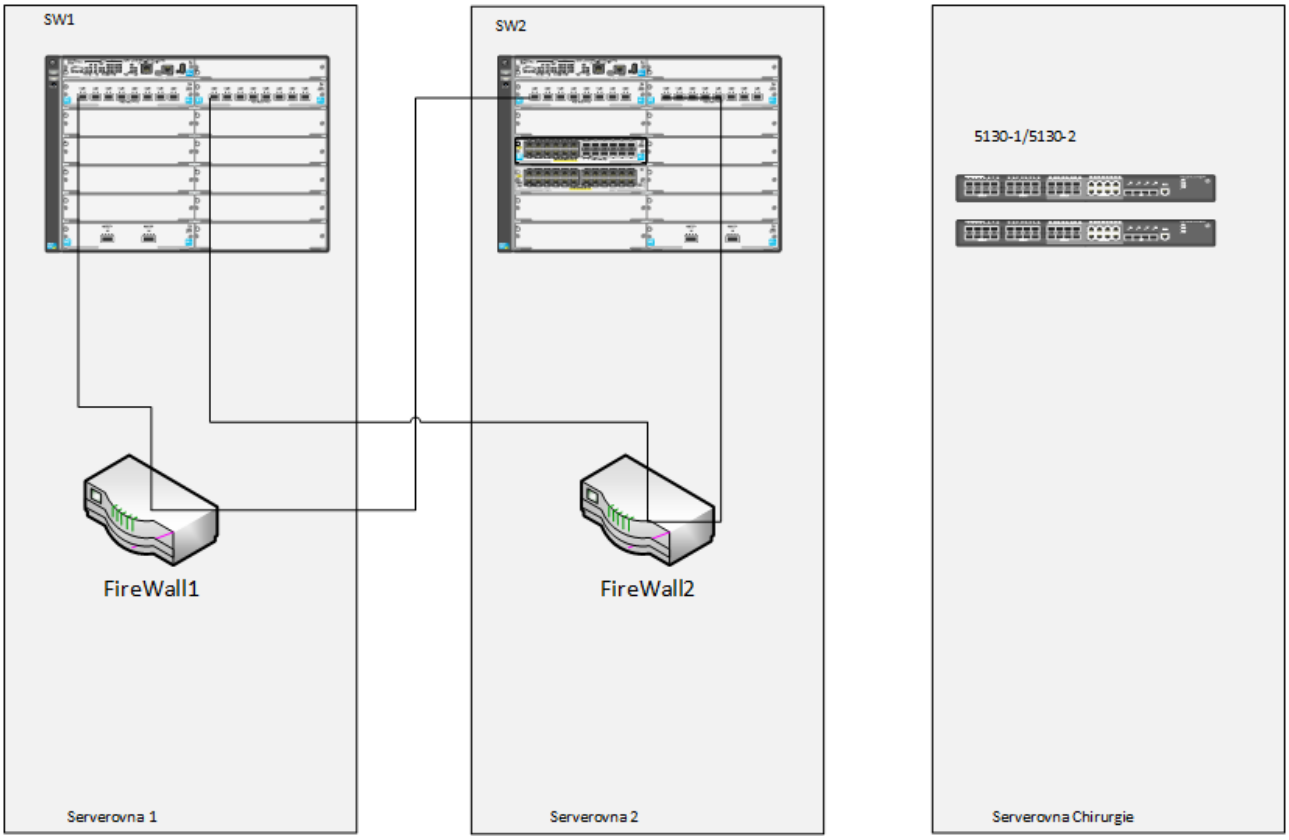
Technická specifikace

1. Cíl projektu

Cílem veřejné zakázky je náhrada stávajících ochran moderním uceleným řešením, kdy jednotlivé prvky ochrany spolu automatizovaně komunikují a spolupracují s cílem zvýšení účinnosti.

Jsou požadovány dva spolupracující fyzické firewally v HA režimu, ochrana elektronické pošty, ochrana publikovaných webových aplikací, webového internetového provozu z koncových zařízení, ochrana koncových bodů (PC a servery – antivirus, synchronizovaná bezpečnost) a systém pro centralizované logování uvedených ochran poskytující i analytické nástroje.

Schéma cílového stavu:



Nově dodávané firewally budou umístěny v serverovnách 1 a 2.

Zadavatel požaduje, aby firewally byly konfigurované v režimu aktiv-aktiv a tomuto režimu musí odpovídat i dodané licence.

Dodávka zahrnuje potřebný HW, licence, drobný a spojovací materiál. Taktéž jsou součástí dodávky implementační a dokumentační práce.

Zadavatel provozuje kritický informační systém, ve kterém nesmí dojít k neplánovaným výpadkům. Proto je dodavatel povinen plánovat a realizovat všechny práce, které mohou dostupnost

informačního systému ohrozit, na dobu mimo hlavní pracovní dobu (víkendy nebo pozdní odpolední hodiny) a především po dohodě se zadavatelem a v termínech jím schválených.

2. Požadovaná dodávka hardware a software

Položka č.	Typ prvku	Umístění	Počet	Specifikace
1.	Firewall (fyzické hardwarové zařízení)	1x Datacentrum S1, 1x Datacentrum S2	2 ks	viz kapitola 4.1
2.	Ochrana elektronické pošty – bezpečná emailová brána (virtual appliance)	1x ve virtualizaci v datacentrech S1 a S2	1 ks	viz kapitola 4.2
3.	Ochrana publikovaných webových aplikací (virtual appliance)	1x ve virtualizaci v datacentrech S1 a S2	1 ks	Viz kapitola 4.3
4.	Ochrana webového internetového provozu z koncových zařízení – proxy (virtual appliance)	1x ve virtualizaci v datacentrech S1 a S2	1 ks	viz kapitola 4.4
5.	Ochrana koncových bodů – PC a serverů (software)	Celá organizace	Komplet	Viz kapitola 4.5
6.	Zařízení pro ukládání a korelaci logů z prvků č. 1. až 5. (virtual appliance)	1x ve virtualizaci v datacentrech S1 a S2	1 ks	viz kapitola 4.6

Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící = nesmí být označeny jako End of Sale nebo End of Support apod.

Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

3. Požadovaná dodávka prací (instalace, konfigurace, uvedení do provozu)

Práce
1. Fyzická montáž firewallů a redundatní propojení s páteřními switchi 2. Instalace virtuálních apliancí pro další části systému 3. Registrace všech licencí a SW komponent na web výrobce se správnými údaji koncového zákazníka 4. Upgrade firmware na poslední dostupné stabilní verze 5. Vytvoření potřebných spojovacích sítí a VLAN 6. Vytvoření HA clusteru fyzických FW boxů 7. Analýza stávajících pravidel a politik na současném FG60E, navržení úprav pro nové prostředí 8. Import pravidel a jejich modifikace dle předchozí analýzy 9. Vytvoření systémových administrátorských účtů a jejich zabezpečení 10. Integrace s AD 11. Vytvoření kontextů pro inter VLAN firewalling a internet firewalling 12. Vytvoření VPN přístupu, zabezpečení, příprava konfigurace pro klienty, konfigurace přístupových politik 13. Konfigurace ochrany mail systému, přizpůsobení pravidel pro filtraci 14. Nasazení proxy serveru, analýza nastavení stávajícího proxy serveru, modifikace pro nové prostředí a nastavení pravidel. Integrace proxy serveru s MS AD pro řízení přístupu na internet dle členství ve skupinách v AD. 15. Nasazení ochrany publikovaných aplikací. Navržení vhodného způsoby publikace, součinost s implementací SSO do aplikací 16. Konfigurace klientské aplikace (ochrany koncových bodů), ověření nasazení přes doménové politiky (a nebo jiným vhodným hromadným způsobem) na vzorku 30 počítačů včetně součinnosti dodavatele při nasazování v celé organizaci 17. Nasazení modulu pro sběr logů ze všech bezpečnostních systémů dodávaných v tomto projektu. 18. Předávací testy 19. Dokumentace 20. Zaškolení správců v rozsahu 2 čd 21. Podpora startu ostrého provozu v rozsahu 3 čd 22. Podpora následného provozu formou dotazů a konzultací v rozsahu 2 čd v průběhu 6 měsíců od předání díla.

Výčet požadovaných vlastností dodávaného hardware a software

3.1 Firewall

Název, typové označení	**FortiGate 200F**	
Číslo	**Popis – firewall (fyzické hardwarové zařízení)**	**Splňuje**
	Základní technické požadavky	
1	Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)	ANO
2	Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU	ANO
3	Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu	ANO

4	Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.	ANO
5	Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.	ANO
	HW parametry	
6	Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x	ANO
7	Počet GE SFP min 8x	ANO
8	Počet 10 GE SFP+ min 4x	ANO
9	Konzolový port pro management	ANO
10	Dedikovaný port RJ45 pro management	ANO
11	Dedikovaný port RJ45 pro HA konfiguraci	ANO
12	USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu	ANO
13	Redundantní napájecí zdroj	ANO
	Výkonnostní parametry	
14	Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps	ANO
15	Latence firewallu (64 B UDP paket) - max 5 mikro sec	ANO
16	Počet naráz otevřených spojení – min 2,7 M	ANO
17	Počet nových spojení za sekundu - min. 260 000	ANO
18	Počet firewall pravidel až 10 000	ANO
19	Podpora virtualizace (min 10 virtuálních kontextů)	ANO
	Network a High Availibility	
20	Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru	ANO
21	Režim fungování L2 – transparentní režim, L3 – NAT/Router	ANO
22	Podpora VLAN	ANO
23	Podpora multicast, vytváření politiky pro multicast routování	ANO
24	Podpora 802.3ad link aggregation	ANO
25	Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading	ANO
26	Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace	ANO
27	Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP	ANO
28	Policy-based routing	ANO
29	Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky	ANO
	VPN	
	- **VPN – Funkce SSL VPN**	
30	Podpora klientského i bezklientského (portálového) režimu	ANO
31	Minimální počet současně navázaných SSL VPN tunelů: 450	ANO
32	Minimální propustnost SSL VPN: 1900Mbps	ANO
	- **VPN - Funkce IPSEC VPN**	
33	podpora site-to-site VPN	ANO
34	podpora klientských VPN	ANO
35	dostupnost VPN klienta pro koncové stanice (Windows, MacOS)	ANO

36	funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů. V opačném případě požadujeme dodání neomezené licence.	ANO
37	Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 2300	ANO
38	Minimální počet klientských IPSEC VPN tunelů: 15000	ANO
39	propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256)	ANO
40	podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování	ANO
41	podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování	ANO
42	podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace	ANO
	- **VPN obecně**	
43	Podpora VXLAN	ANO
44	Podpora L2TP, PPTP, GRE	ANO
45	podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec	ANO
	Token pro dvoufaktorové ověření	
46	150 licencí tokenů pro ověření druhým faktorem pro přístup přes VPN. Požadované vlastnosti: podpora Android, iOS, Windows 10	ANO
	UTM	
	- **UTM – Funkce detekce aplikací na L7 (Application Control)**	
47	Detekce známých aplikací na základě signatur	ANO
48	Signaturový database automaticky aktualizované výrobcem	ANO
49	alespoň 4000 podporovaných aplikací	ANO
50	pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)	ANO
51	možnost tvorby vlastních signatur	ANO
52	detekované aplikace je možné: povolit, monitorovat, blokovat	ANO
53	na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci	ANO
54	funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.	ANO
	- **UTM – Funkce detekce a potlačení narušení (IPS/IDS)**	
55	signatury automaticky aktualizované výrobcem	ANO
56	alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem	ANO
57	možnost tvorby vlastních signatur	ANO
58	funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům	ANO
59	propustnost funkce IPS včetně logování min. 4800Mbps (měřeno na komunikaci typu mix aplikací)	ANO
	- **UTM – Funkce antivirové kontroly**	
60	Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem	ANO
61	Signatury automaticky aktualizované výrobcem	ANO
62	požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)	ANO
63	možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce	ANO
64	deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2900 Mbps	ANO
65	funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům	ANO
66	Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od	ANO

	poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů	
67	Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.	ANO
	- **UTM – Funkce kategorizace webových stránek**	
68	založená na centrálně spravované databázi výrobce	ANO
69	minimálně 50 filtračních kategorií	ANO
70	možnost definice vlastních kategorií	ANO
71	možnost definice vlastních seznamů zakázaných URL	ANO
72	kategorizace musí zahrnovat I české a slovenské internetové stránky	ANO
	- **UTM – Funkce DNS filtru**	
73	Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)	ANO
74	Možnost definovat vlastní tzv. blacklist domén	ANO
75	Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL	ANO
76	Možnost importu seznamu blokovaných domén do DNS filtru	ANO
77	Detekce a blokování komunikace do botnet sítí	ANO
	- **UTM - Funkce ochrany před únikem citlivých informací (DLP)**	
78	možností analýzy běžných typů dokumentů a protokolů	ANO
79	možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum	ANO
	- **UTM obecně**	
80	Email filter - jednoduchá antispamová a antivirová inspekce elektronické pošty	ANO
81	Podpora SSL dekrypce/SSL inspekce s minimální propustností 3900Mbps	ANO
82	DoS Policy prevence proti základním útokům typu DoS	ANO
83	Firewall musí být vybaven bezpečnostním modulem pro ukládání citlivých informacích založeným na bázi HW (TPM)	ANO
	Firewall	
84	Možnost nastavovat firewall politiku na základě geografických údajů	ANO
85	Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem	ANO
86	Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud	ANO
87	Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru	ANO
88	Viditelnost do provozu na aplikační úrovni	ANO
89	Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo)	ANO
90	Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu	ANO
91	Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.	ANO
92	Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii	ANO
93	Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu	ANO
94	Podpora funkce reverzní proxy	ANO

95	Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů	ANO
	- **Firewall – Explicit proxy**	ANO
96	podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)	ANO
97	podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos	ANO
98	funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta	ANO
99	Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru	ANO
	Virtualizace	
100	Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.	ANO
101	Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)	ANO
102	Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	ANO
	Management	
103	FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici	ANO
104	Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě	ANO
105	Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	ANO
	Záruka a podpora	ANO
106	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, záruku na HW, to vše po dobu 5 let.	ANO

3.2 Ochrana elektronické pošty – bezpečná emailová brána

Název, typové označení	**FortiMail-VM02**	
Číslo	**Popis – Ochrana elektronické pošty – bezpečná emailová brána (VM appliance)**	**Splňuje**
	Základní technické požadavky	
1	Provedení VM appliance v prostředí VMware ESXi	ANO
	HW požadavky	
2	Podpora až 4 sítových rozhraní v rámci síťového prostředí hypervisoru	ANO
3	Podpora VMware ESXi	ANO
4	VM appliance je schopno používat nejméně 2 vCPU	ANO
5	VM appliance je schopno používat nejméně 8 GB paměti	ANO
6	VM appliance je schopno používat nejméně 2 TB diskového prostoru	ANO
	Funkční požadavky	
7	Možnost nasazení v režimu MTA gateway nebo transparetní režim	ANO
8	Možnost nasazení v režimu vysoké dostupnosti (včetně sdílení fronty) pro budoucí rozšíření	ANO

9	Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky (NG Firewall, sandbox) za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách (škodlivém kódu) sandboxovací technikou.	ANO
10	Ochrana proti škodlivému kódu, nevyžádané elektronické poště a uniku citlivých dat	ANO
11	Podpora víceúrovňové detekce nevyžádané pošty (IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza)	ANO
12	reakce na detekovaný spam minimálně: přidání tagu, přidání hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce	ANO
13	Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky)	ANO
14	Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant škodlivého kódu, odstranění aktivního obsahu PDF a kancelářských dokumentů, karanténa, odstranění škodlivých odkazů z emailů, AV kontrola musí být plně integrována s platformou Sandbox (viz níže), umožňující pokročilou ochranu před pokročilými typy hrozeb včetně tzv. zero- day útoků. Na rozdíl od firewallu tato integrace musí být v režimu pozdržení emailu ve frontě až do konce analýzy na sandboxu, sdílení signatur dynamicky vytvářených na platformě sandbox	ANO
15	Podpora IPv6	ANO
16	Podpora VLAN	ANO
17	Plnohodnotná integrace s LOG serverem a SIEM platformou.	ANO
18	Plnohodnotná integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem)	ANO
	Výkonové požadavky	
19	Propustnost min. 50 000 emailů za hodinu při průměrné velikosti email ~100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu	ANO
20	Podpora ochrany minimálně 100 emailových domén	ANO
21	Licenčně nezávislý model na počtu uživatelů, mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek)	ANO
	Deklarace	
22	Certifikace VB verified spam +	ANO
23	Certfikiace VB 100 Virus	ANO
24	Certifikace ICSA labs	ANO
25	Certifikace AAA SE Labs	ANO
	Záruka a podpora	ANO
26	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let.	ANO

3.3 Ochrana publikovaných webových aplikací

Název, typové označení	**FortiWeb VM01**	
Číslo	**Popis – Ochrana publikovaných webových aplikací (VM appliance)**	**Splňuje**
	Základní technické požadavky	
1	Provedení VM appliance v prostředí VMware ESXi	ANO
2	Propustnost minimálně 25Mbit	ANO
3	Podpora minimálně 10 virtuálních síťových rozhraní	ANO
	Topologie nasazení	
4	Reverzní proxy	ANO
5	Transparentní proxy	ANO
	Ochrana webového protokolu	
6	AI-based Machine Learning	ANO
7	Automatic profiling (white list)	ANO
8	Web server and application signatures (black list)	ANO
9	IP address reputation	ANO
10	IP address geolocation	ANO
11	HTTP RFC compliance Native support for HTTP/2	ANO
12	WebSocket protection and signature enforcement	ANO
13	Man in the Browser (MiTB) protection	ANO
	Ochrana aplikací	
14	Ochrana/kontrola dle OWASP Top 10	ANO
15	ochrana před Cross Site Scripting	ANO
16	ochrana Cross Site Request Forgery	ANO
17	ochrana před Session Hijacking	ANO
18	vestavěný Vulnerability Scanner	ANO
19	Kontrola nahrávaných souborů vestavěným AV skenerem a pomocí sandboxu.	ANO
	Bezpečnostní funkce	
20	Rozpoznávání aplikací dle signatur	ANO
21	Kontrola shody XML and JSON protokolů se standardem	ANO
22	Detekce Malware	ANO
23	Oprava chybných webových požadavků za běhu (Virtual patching)	ANO
24	Validace síťových a aplikačních protokolů	ANO
25	Ochrana před útoky hrubou silou	ANO
26	Cookie signing and encryption	ANO
27	Syntax-based SQLi detection	ANO
28	Ochrana HTTP hlaviček	ANO
29	Custom error message and error code handling	ANO
30	Ochrana OS rozpoznáváním signatur ohrožení	ANO
31	Ochrana před známými útoky a 0-day útoky	ANO
32	L4 Stateful Network Firewall	ANO
33	Prevence DoS	ANO
34	Rozšířená ochrana korelací více bezpečnostních prvků	ANO
35	Ochrana před únikem dat	ANO

	Podpora Web aplikací	
36	Layer 7 server load balancing	ANO
37	URL Rewriting	ANO
38	Content Routing	ANO
39	HTTPS/SSL Offloading	ANO
40	HTTP Compression	ANO
41	Caching	ANO
	Podpora autentikace	
42	Aktivní a pasivní autentikace web aplikací	ANO
43	Site Publishing and SSO	ANO
44	RSA Access for 2-factor authentication	ANO
45	LDAP, RADIUS, and SAML support	ANO
46	SSL client certificate support	ANO
47	CAPTCHA and Real Browser Enforcement (RBE)	ANO
	Záruka a podpora	
48	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let.	ANO

3.4 Ochrana webového internetového provozu z koncových zařízení – proxy

Název, typové označení	**FortiProxy-VM02**	
Číslo	**Popis – Ochrana webového internetového provozu z koncových zařízení – proxy (VM appliance)**	**Splňuje**
	Základní technické požadavky	
1	Provedení VM appliance v prostředí VMware ESXi	ANO
2	Podpora minimálně 500 současně pracujících uživatelů	ANO
3	Podpora minimálně 10 virtuálních síťových rozhraní	ANO
	Topologie nasazení	
4	Explicitní proxy	ANO
5	Transparentní proxy	ANO
6	Forward proxy	ANO
	Požadovaná ochrana	
7	Integrace se službou threat intelligence service a online aktualizace signatur v reálném čase	ANO
8	Integrace s cloudovým sandboxem	ANO
9	Všechny bezpečnostní funkce jsou vestavěny – není třeba dalších apliancí pro provoz	ANO
	- **DNS and Web filtrace**	
10	Dynamická kategorizace webových stránek	ANO
11	Blokování podezřelých a škodlivých web stránek a URL	ANO
12	Statický systém white a black listů	ANO
	- **Aplikační kontrola**	
13	Detailní řízení přístupu pro sociální sítě	ANO
14	Podpora více jak 3000+ aplikací	ANO

	- **Požadovaná ochrana - ostatní**	
15	Antivirus a DLP	ANO
16	Analýza obsahu	ANO
17	IPS signatury a filtry	ANO
18	SSL/SSH Inspekce	ANO
19	Možnost uživatelských aplikačních signatur	ANO
	Ověřování uživatelů	
20	Podpora různých ověřovacích způsobů a protokolů, minimálně: Radius, SAML, LDAP, NTLM, Kerberos	ANO
21	Vestavěné ověřovací funkce nevyžadují dodatečné zařízení/licence	ANO
	Záruka a podpora	
22	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let.	ANO

3.5 Ochrana koncových bodů

Název, typové označení	**FortiClient**	
Číslo	**Popis – Ochrana koncových bodů (software)**	**Splňuje**
	Požadované parametry, vlastnosti	
1	Produkt musí pokrýt 500 koncových zařízení + 50 serverů, licence musí jít rozšířit min. na 5000.	ANO
2	Produkt musí být integrovatelný a synchronizovatelný s adresářovou službou Active Directory (AD)	ANO
3	Produkt musí zajistit informovanost o koncových bodech, soulad s požadavky a uplatňování pravidel díky předávání telemetrických údajů bez ohledu na umístění zařízení – ať se nachází v sídle zadavatele nebo v kavárně.	ANO
4	Produkt musí automatizovat prevenci známých i dosud neznámých hrozeb pomocí vestavěných bezpečnostních funkcí a spoluprací s nabízeným NGFW řešením.	ANO
5	Ochrana proti známým hrozbám – bezpečnostní funkce řešení musí zahrnout minimálně antivirové jádro, aplikační firewall, skener zranitelností s automatickými opravami a filtrování internetového provozu. Součinností těchto funkcí musí jít omezit prostor pro útok a blokovat polymorfní i běžný škodlivý software a známé typy útoků proti koncovým bodům z různých směrů.	ANO
6	Ochrana proti neznámým hrozbám – řešení musí automatizovat předávání neznámých objektů zařízení typu „iSandbox“, které se pokusí o detekci pomocí ověření kontrolního otisku neznámého souboru nebo provede dynamickou analýzu k odhalení případného škodlivého chování. Pokročilý škodlivý software a tzv. hrozby nultého dne jsou potlačeny pomocí sdílených bezpečnostních informací, na jejichž základě nabízené řešení automaticky izoluje příslušný objekt a imunizuje všechny ostatní koncové body.	ANO
7	Řešení bude obsahovat centrální prvek, server pro správu, který umožní komplexní zavedení ochrany u všech koncových zařízení, jejich registraci, správu a sledování. Centrální prvek musí být On-premise, zadavatel nepřipouští cloudovou centrální správu.	ANO
8	Centrálně bude možno na koncových zařízeních spravovat antivirus, zabezpečení přístupu k internetu, vzdálený přístup (IPsec a SSL VPN), aplikační firewall, skenování zranitelností a související pokročilé funkce.	ANO
9	Na dálku bude možno také spustit antivirovou kontrolu a izolovat infikovaná koncová zařízení.	ANO
10	Produkt musí být integrovatelný s nabízeným řešením pro ukládání a korelaci logů	ANO
	Záruka a podpora	ANO

11	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let.	ANO

3.6 Zařízení pro ukládání a korelaci logů

Název, typové označení	**FortiAnalyzer VM**	
Číslo	**Popis – Zařízení pro vyhodnocování a analýzu logů (VM appliance)**	**Splňuje**
	Požadované parametry, vlastnosti	
1	Zařízení musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem.	ANO
2	Zařízení musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.	ANO
3	Musí se jednat o virtuální appliance s podporou minimálně VMware, KVM a Hyper-V	ANO
4	Kapacita úložiště logů minimálně 500GB a minimální limit pro množství přijatých logů za jeden den 11GB	ANO
5	Podpora minimálně 4 virtuálních interfaců	ANO
6	Možnost škálovatelného navýšení kapacity úložiště na základě licence	ANO
7	Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma	ANO
8	Mít možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě	ANO
	Multitenantnost	
9	Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení)	ANO
10	Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků	ANO
	Logovací funkce	
11	Musí se jedna o centrální logovací prvek pro všechny UTM firewally a všechny technologie dodávané v rámci tohoto projektu.	ANO
12	Musí umět ukládat jakkoliv Syslog zprávy	ANO
13	Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites	ANO
14	Vizualizace provozu nad všemi firewally	ANO
15	Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy	ANO
16	Realtime a historický náhled do logů	ANO
17	Korelace logů	ANO
18	Samostatná sekce týkající se hrozeb v síti	ANO
19	Podpora prohlížení statistických údajů nad logy	ANO
	Reporting	
20	Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF	ANO
21	Generování reportů v pravidelných intervalech	ANO
22	Předefinované vzory pro reporty na nejčastější použití	ANO
23	Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze	ANO
24	Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky	ANO
	Další funkce	
25	Event Management - upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou	ANO

26	Předvytvořený dashboard pro využití dohledovým centrem	ANO
27	Možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace	ANO
	Možnosti správy a komunikace	
28	Podpora SNMPv2, SNMPv3	ANO
29	Podpora REST API	ANO
30	Správa přes webové rozhraní HTTPS	ANO
31	Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)	ANO
32	Podpora statického routování	ANO
33	Možnost zašifrování spojení mezi zařízením, které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace	ANO
	Záruka a podpora	ANO
34	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let.	ANO

3.7 Ostatní podmínky

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

4. Předávací kritéria

- Veškerý HW a SW je dodaný, HW je namontovaný a instalovaný
- Veškerý HW i SW je nakonfigurovaný, funkčnost ověřena během v ostrém provozu
- Test automatického přepnutí provozu při odpojení firewallu
- Test zranitelností na veřejném rozhraní firewallu
- Dokumentace je předána a odpovídá realitě