Kupní smlouva

uzavřená dle zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jako „**Občanský zákoník**“ nebo „**OZ**“).

Číslo smlouvy prodávajícího:
Číslo smlouvy kupujícího: 2020001926

uzavřená mezi

společnost **BIT SERVIS spol. s r.o.**
se sídlem Libušská 144/252, 142 00 Praha 4
IČO: 45793972
DIČ: CZ45793972
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 11262
Zastoupená: Ondřej Koutský, jednatel
bank. spojení: Česká spořitelna a.s.
číslo účtu: [redacted]

(dále také „**prodávající**“)

a

Statutární město České Budějovice
se sídlem nám. Přemysla Otakara II. 1/1; 370 92 České Budějovice
IČO: 002 44 732
DIČ: CZ 002 44 732
zastoupené: Ing. Jiřím Svobodou, primátorem
bank. spojení: Česká spořitelna, a.s.
číslo účtu: [redacted]

(dále také „**kupující**“)

Článek 1.
Předmět smlouvy

1.1. Tato smlouva je uzavírána na základě veřejné zakázky s názvem: „NextGeneration Firewally pro LAN statutárního města České Budějovice“.

1.2. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu předmět koupě a provést instalační služby dle zadávací dokumentace k veřejné zakázce a **Přílohy č. 1** této smlouvy (dále jen „Zboží“) a rovněž poskytnout veškeré doklady týkající se Zboží (například návody k obsluze v českém jazyce či záruční listy, instalační protokoly,…), a to za podmínek této smlouvy, a závazek kupujícího zaplatit za dodané Zboží prosté vad a řádně provedené služby sjednanou kupní cenu.

Článek 2.
Kupní cena, platební podmínky

2.1. Smluvní strany sjednávají celkovou cenu za dodávku Zboží na základě této smlouvy ve výši **2 621 398,-Kč** (slovy: dva miliony šest set dvacet jedna tisíc tři sta devadesát osm korun českých) bez DPH. Ke sjednané ceně bude připočtena daň z přidané hodnoty ve výši stanovené právními předpisy platnými v době uskutečnění zdanitelného plnění. Celková cena vychází z položkových cen uvedených v **Příloze č. 1** této smlouvy.

2.2. Sjednaná celková cena je nejvýše přípustná a zahrnuje v sobě veškeré náklady, které má prodávající se splněním závazků z této smlouvy.

2.3. Kupující se zavazuje zaplatit sjednanou celkovou cenu, včetně příslušné daně z přidané hodnoty na základě faktury – daňového dokladu vystaveného prodávajícím, ve lhůtě splatnosti uvedené ve faktuře – daňovém dokladu. Faktura – daňový doklad bude prodávajícím vystaven tak, že bude splňovat náležitosti dle platných právních předpisů. Celková cena, včetně příslušné daně z přidané hodnoty, bude uhrazena bezhotovostním převodem na účet prodávajícího uvedený ve vystavené faktuře – daňovém dokladu. Faktura – daňový doklad bude vystaven po podpisu dodacího listu a/nebo akceptačního (předávacího) protokolu.

2.4. Splatnost faktury – daňového dokladu sjednávají smluvní strany v délce 30 dnů ode dne jejího doručení kupujícímu.

2.5. V případě, že daňový doklad bude trpět formálními (absence zákonných náležitostí faktury, apod.) či věcnými (cena neodpovídá nabídce, práce nebyly provedeny či byly provedeny vadně apod.) vadami, je kupující povinen prodávajícího na tyto vady upozornit a tuto prodávajícímu vrátit k přepracování. Lhůta splatnosti v daňovém dokladu uvedená, se tímto oznámením přerušuje do doby odstranění vad daňového dokladu. Po odstranění sporných záležitostí pak započne běžet nová lhůta pro zaplacení nově vystaveného daňového dokladu v délce dle odst. 2.4. tohoto článku.

Článek 3.
Místo dodání, termín dodání, předání a převzetí

3.1. Prodávající se zavazuje Zboží dodat na adresu sídla kupujícího (dále též jako „**Místo dodání**“) do padesáti kalendářních dnů ode dne účinnosti této smlouvy (v této smlouvě též jako „**Termín dodání**“). V Termínu dodání a Místě dodání bude provedena instalace v souladu s **Přílohou č. 1** této smlouvy. Prodávající v Místě dodání a Termínu dodání Zboží předá kupujícímu.

3.2. Kupující se zavazuje Zboží v Místě dodání a Termínu dodání od prodávajícího převzít a převzetí potvrdit písemně podpisem dodacího listu a instalačních protokolů. V případě, že kupující nepotvrdí převzetí Zboží/provedení instalace, bude o tom učiněn záznam. Osobou oprávněnou jednat za kupujícího při převzetí Zboží a podpisu dodacího listu a instalačních protokolů je vedoucí odboru informačních a komunikačních technologií Magistrátu města České Budějovice nebo jím pověřená osoba.

3.3. Kupující se zavazuje poskytnout prodávajícímu veškerou nezbytnou součinnost pro předání Zboží v Místě dodání a v Termínu dodání, a dále nezbytnou součinnost ke splnění jakéhokoliv závazku prodávajícího založeného touto smlouvou. O dobu prodlení kupujícího s poskytnutím jakékoliv součinnosti se posouvá Termín dodání.

3.4. Prodávající je oprávněn dodat Zboží před sjednaným Termínem dodání. Odst. 3.2. tohoto článku se v takovém případě bude aplikovat obdobně.

3.5. V případě, že dojde k neodvratitelné události, kterou je vyšší moc, vyšší zásahy, stávky, výluky, přírodní katastrofy, působení přírodních živlů, včetně takové neodvratitelné události u dodavatele prodávajícího, která byť jen částečně znemožňuje splnění závazku prodávajícího dodat Zboží, upozorní prodávající na uvedené kupujícího a sdělí mu předpokládanou dobu zdržení dodání. O skutečnou dobu zdržení dodání dojde k prodloužení Termínu dodání. O objektivnosti důvodů dle tohoto odstavce je oprávněn rozhodnout výhradně kupující. Nebude-li kupujícím rozhodnuto o objektivnosti důvodů, nemá prodávající nárok na prodloužení Termínu dodání.

Článek 4.
Kontrola Zboží, Odpovědnost za vady

4.1. Prodávající poskytuje na Zboží rozšířenou záruku dle specifikace předmětu plnění v **Příloze č. 1** od data převzetí Zboží kupujícím.

4.2. Prodávající poskytuje kupujícímu záruku, že Zboží bude nejméně po záruční dobu způsobilé k použití pro ujednaný, jinak obvyklý, účel, a že si zachová ujednané, jinak obvyklé, vlastnosti.

4.3. Pro oznámení jakékoliv vady na Zboží platí, že kupující se zavazuje oznámit vadu prodávajícímu řádným písemným oznámením doručeným prodávajícímu. Kupující se zavazuje oznámit prodávajícímu veškeré vady dodaného Zboží v přiměřené době, a to nejpozději ve lhůtě 7 dnů od dodání Zboží, v případě zjevných vad, nebo 7 dnů od zjištění vady, v případě skrytých vad. Oznámení vad musí být ve lhůtě podle předcházející věty

prokazatelně odesláno prodávajícímu. Prodávající se po dobu záruky zavazuje řádně vytknutou vadu bezplatně odstranit do 30 dnů od jejího oznámení.

Článek 5.
Odstoupení od smlouvy

5.1. Prodávající je oprávněn odstoupit od této smlouvy v kterémkoliv z následujících případů:
a) kupující bude v prodlení se zaplacením Celkové ceny, včetně příslušné daně z přidané hodnoty, po dobu alespoň třiceti dnů,
b) kupující bude v prodlení s převzetím Zboží po dobu alespoň pěti dnů,
c) kupující bude v prodlení s poskytnutím jakékoliv součinnosti podle článku 3 odst. 3.3. nebo 3.4. této smlouvy po dobu alespoň pěti dnů,

5.2. Kupující je oprávněn odstoupit od této smlouvy v kterémkoliv z následujících případů:
a) prodávající bude v prodlení s předáním Zboží v Termínu dodání a Místě dodání po dobu alespoň deseti dnů,
b) v případě zjištění jakéhokoliv nesouladu funkčnosti Zboží kdykoli v době záruky s technickými požadavky zadávací dokumentace,
c) v případě zjištění, že Zboží nepochází z oficiální distribuce výrobce pro Českou republiku, nebo není v EU servisovatelné autorizovaným servisem.

5.3. Odstoupení od této smlouvy musí být písemné a musí být doručeno druhé smluvní straně. Smlouva se ruší ke dni doručení odstoupení druhé smluvní straně a smluvní strany jsou povinny vrátit si na základě této smlouvy poskytnuté plnění. Odstoupení od smlouvy nemá vliv na právo oprávněné smluvní strany na náhradu škody ani smluvní pokutu.

Článek 6.
Smluvní pokuty

6.1 Kupující se v případě jeho prodlení se zaplacením Celkové ceny, včetně DPH, zavazuje zaplatit prodávajícímu smluvní úrok z prodlení ve výši 0,02 % z dlužné částky bez DPH, a to za každý i započatý den prodlení.

6.2 Prodávající se zavazuje zaplatit kupujícímu smluvní pokutu ve výši 0,2 % z Celkové ceny sjednané v článku 2 odst. 2.1. této smlouvy bez DPH, a to za každý i započatý den prodlení s dodáním Zboží.

6.3 V případě, že prodávající bude v prodlení se lhůtou pro odstranění vad uplatněných kupujícím v záruční době dle čl. 4 odst. 4.3. této smlouvy, je prodávající povinen kupujícímu zaplatit smluvní pokutu ve výši 10.000,- Kč, a to za každý započatý den prodlení a každou jednotlivou vadu.

6.4 Zaplacením smluvní pokuty není dotčeno právo na náhradu škody způsobené porušením povinnosti i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta, a to i ve výši přesahující smluvní pokutu. Náhrada škody zahrnuje skutečnou škodu a ušlý zisk.

Článek 7.
Další povinnosti prodávajícího

7.1 Prodávající je povinen respektovat níže uvedené podmínky, vyplývající ze skutečnosti, že Zboží bude spolufinancováno z Evropských strukturálních a investičních fondů (Evropský fond pro regionální rozvoj – integrovaný regionální operační program) v gesci Ministerstva pro místní rozvoj České republiky a plnit tyto povinnosti:

7.1.1. archivovat originální vyhotovení smlouvy včetně jejích dodatků, originály účetních dokladů a dalších dokladů vztahujících se k realizaci Dodávky, a to po dobu 10 let od zániku této smlouvy, nejméně do roku 2028.

7.1.2. zajistit, aby každý originál účetního dokladu byl označen číslem projektu a obsahoval informaci, že se jedná o projekt financovaný z Evropských strukturálních a investičních fondů v rámci Integrovaného regionálního operačního programu pro období 2014-2020.

7.1.3. Prodávající souhlasí dle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, s výkonem kontroly na předmět zakázky a zavazuje se minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, Auditního orgánu, Platebního a certifikačního orgánu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy). Prodávající je dále povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

7.2 V případě, že z důvodu porušení smluvní povinnosti prodávajícího dle tohoto článku bude kupujícímu uložena kontrolním orgánem veřejné správy jakákoliv sankce, zavazuje se prodávající částku ve výši uložené sankce kupujícímu nahradit.

Článek 8.
Závěrečná ujednání

8.1 Tato smlouva nabývá platnosti dnem podpisu poslední ze smluvních stran a účinnosti dnem zveřejnění v registru smluv dle zákona č. 340/2015 Sb., v platném znění.

8.2 Tato smlouva může být měněna pouze formou písemných dodatků podepsaných oprávněnými zástupci obou stran.

8.3 V případě, že kterékoli ustanovení této smlouvy se stane nebo bude shledáno neplatným, neúčinným, nezákonným či nevynutitelným a lze jej oddělit od ostatních ustanovení této smlouvy, zůstávají ostatní ustanovení smlouvy nadále nedotčena. Smluvní strany se tímto zavazují, že nahradí neplatné, neúčinné, nezákonné či nevynutitelné ustanovení ustanovením platným, účinným, zákonným a vynutitelným tak, aby nahrazené ustanovení odpovídalo účelu původnímu ustanovení a této smlouvě, případně zpracují a uzavřou odpovídající novou platnou smlouvu.

8.4 Smluvní strany se dohodly na místní příslušnosti soudu v souladu s ustavením § 89a zákona č. 99/1963 Sb., občanský soudní řád, v platném znění takto: Místně příslušným soudem pro případ sporů vyplývajících z této smlouvy je soud příslušný dle sídla kupujícího.

8.5 Tato smlouva je smluvními stranami uzavírána výlučně v elektronické podobě, a to připojením uznávaného elektronického podpisu zástupců smluvních stran.

8.6 Smluvní strany berou na vědomí, že za podmínek vyplývajících ze zákona č. 340/2015 Sb., v platném znění, podléhá tato smlouva uveřejnění v registru smluv, přičemž uveřejnění dle tohoto zákona zajistí kupující způsobem, v rozsahu a ve lhůtách z něho vyplývajících. Smluvní strany si ujednávají, že kupující je oprávněn bez omezení provést uveřejnění úplného znění této smlouvy včetně všech příloh v registru smluv i v případě, že povinnost k jejímu uveřejnění ze zákona dle předchozí věty nevyplývá, jakož i uveřejnění na oficiálních webových stránkách města České Budějovice. Smluvní strany berou dále na vědomí, že kupující je povinen tuto smlouvu či skutečnosti z ní vyplývající uveřejnit nebo poskytnout třetím osobám, pokud takový postup vyplývá z příslušných právních předpisů. Pro účely uveřejňování či poskytování dle předchozích vět smluvní strany současně shodně prohlašují, že žádnou část této smlouvy nepovažují za své obchodní tajemství bránící jejímu uveřejnění či poskytnutí. Ujednání dle tohoto odstavce se vztahují i na všechny případné dodatky k této smlouvě, jejichž prostřednictvím je tato smlouva měněna či ukončována.

8.7 Vyhrazená změna závazku:

8.7.1. Kupující si v souladu s § 100 odst. 2 zákona č. 134/2016 Sb., v platném znění, vyhrazuje v případě naplnění některé z podmínek pro odstoupení smluvní strany stanovené v čl. 5 této smlouvy změnu prodávajícího v průběhu plnění veřejné zakázky a jeho nahrazení účastníkem zadávacího řízení, který se dle výsledku hodnocení umístil druhý v pořadí, a to za cenových podmínek obsažených v nabídce tohoto v pořadí druhého účastníka zadávacího řízení v souladu se závazným návrhem smlouvy dle zadávací dokumentace.

8.7.2. Pokud účastník zadávacího řízení, který se dle výsledků hodnocení umístil druhý v pořadí, odmítne poskytovat plnění namísto původně vybraného prodávajícího za podmínek uvedených v předchozím odstavci, je kupující oprávněn obrátit se na účastníka zadávacího řízení, který se umístil jako třetí v pořadí.

8.8 Smluvní strany potvrzují, že tato smlouva byla uzavřena svobodně, vážně a na základě projevené vůle obou smluvních stran, že souhlasí s jejím obsahem a jsou si vědomy všech důsledků jejího uzavření. Osoby podepisující za smluvní strany tuto smlouvu prohlašují, že jsou oprávněny smlouvu jménem smluvní strany uzavřít.

8.9 Uzavření této smlouvy bylo schváleno usnesením Rady města České Budějovice č. …….. ze dne ……

8.10 Přílohy ke smlouvě:

Příloha č. 1 – Položková specifikace Zboží včetně cen

Příloha č. 2 – Technické parametry dodávaného Zboží

V Praze dne: 13.8.2020

za prodávajícího

Ondřej Koutský

Digitálně podepsal Ondřej Koutský
DN: cn=Ondřej Koutský, c=CZ, o=BIT SERVIS spol. s r.o., givenName=Ondřej, sn=Koutský, 2.5.4.97=NTRCZ-45793972, serialNumber=ICA - 10414101
Datum: 2020.10.14 11:22:16 +02'00'

BIT SERVIS spol. s r.o.
Ondřej Koutský, jednatel

V Českých Budějovicích dne:

za kupujícího

statutární město České Budějovice
Ing. Jiří Svoboda, primátor

Příloha č. 1 – Položková specifikace Zboží včetně cen

Popis produktu	Název zařízení	Part number	Dodávané množství	Jednotková cena bez DPH	Jednotková cena včetně DPH	Cena celkem bez DPH	Cena celkem včetně DPH	Sazba DPH
NG Firewall – distribuční	Fortigate 100E		0					
Záruka, podpora, technický a aktualizační servis po dobu 5 let		FC-10-FG1HE-950-02	2	92 477,00-Kč	111 897,17-Kč	184 954,00-Kč	223 794,34-Kč	21%
NG Firewall – segmentační	FortiGate 600E, HW only	FG-600E	2	109 987,00-Kč	133 084,27-Kč	219 974,00Kč	266 168,54-Kč	21%
Záložní napájecí zdroj pro NG Firewall-segmentační	AC power supply for FG-600E	SP-FG300E-PS	2	20 619,00-Kč	24 948,99-Kč	41 238,00-Kč	49 897,98-Kč	21%
Propojovací kabely pro NG Firewall-segmentační	10GE SFP+ Passive Direct Attach Cable, 3 m	SP-CABLE-FS-SFP+3	4	1 449,00-Kč	1 753,29-Kč	5 796,00-Kč	7 013,16-Kč	21%
Záruka, podpora, technický a aktualizační servis po dobu 5 let		FC-10-F6H0E-950-02	2	343 439,-Kč	415 561,19-Kč	686 878,00-Kč	831 122,38-Kč	21%
NG Firewall – Zimní stadion	Fortigate 60E		0					
Záruka, podpora, technický a aktualizační servis po dobu 5 let		FC-10-0060E-247-02	1	11 560,00-Kč	13 987,60-Kč	11 560,00-Kč	13 987,60-Kč	21%
NG Firewall – Bazén	Fortigate 60E		0					
Záruka, podpora, technický a aktualizační servis po dobu 5 let		FC-10-0060E-247-02	1	11 560,00-Kč	13 987,60-Kč	11 560,00-Kč	13 987,60-Kč	21%
NG Firewall – Sportovní hala	Fortigate 60F		0					
Záruka, podpora, technický a aktualizační servis po dobu 5 let		FC-10-0060F-247-02	1	12 358,00-Kč	14 953,18-Kč	12 358,00-Kč	14 953,18-Kč	21%
NG Firewall – pro systém CIS	FortiAP 221E	FAP-221E-E	2	6 379,00-Kč	7 718,59-Kč	12 758,00-Kč	15 437,18-Kč	21%
Záruka, podpora, technický a aktualizační servis po dobu 5 let	Je součástí zařízení FortiAP pro NG Firewall – pro systém CIS		0					
NG Firewall – pro mobilní pracoviště	Wall Plate AP - Dual radio 2x2 MU-MIMO), internal	FAP-C24JE-E	3	3 255,00-Kč	3 938,55-Kč	9 765,00-Kč	11 815,65-Kč	21%

Popis produktu	Název zařízení	Part number	Dodávané množství	Jednotková cena bez DPH	Jednotková cena včetně DPH	Cena celkem bez DPH	Cena celkem včetně DPH	Sazba DPH
	antennas							
NG Firewall – pro mobilní pracoviště	AC Power Adaptor	SP-FAP400-PA-EU	3	868,00-Kč	1 050,28-Kč	2 604,00-Kč	3 150,84-Kč	21%
Záruka, podpora, technický a aktualizační servis po dobu 5 let	je součástí zařízení NG Firewall – pro mobilní pracoviště		0					
Centrální management platforma pro správu všech firewallů v síti	FortiManager VM, Virtual Appliance	FMG-VM-Base	1	29 307,00-Kč	35 461,47-Kč	29 307,00-Kč	35 461,47-Kč	21%
Podpora, technický a aktualizační servis po dobu 5 let		FC1-10-M3004-248-02	1	34 464,00-Kč	41 701,44-Kč	34 464,00-Kč	41 701,44-Kč	21%
Bezpečnost koncových stanic	FortiClient Security Fabric Agent with EPP license subscription for 25 endpoints 5YR	FC1-15-EMS01-299-02	24	32 862,00-Kč	39 763,02-Kč	788 688,00-Kč	954 312,48-Kč	21%
Podpora, technický a aktualizační servis po dobu 5 let	je součástí licence pro Bezpečnost koncových stanic		0					
Systém pro centrální ukládání a korelaci logů z firewallů	FortiAnalyzer virtual appliance		0					
Systém pro centrální ukládání a korelaci logů z firewallů	FortiAnalyzer VM, 1 GB Logs/Day Add-on	FAZ-VM-GB1	4	10 344,00-Kč	12 516,24-Kč	41 376,00-Kč	50 064,96-Kč	21%
Systém pro centrální ukládání a korelaci logů z firewallů	FortiAnalyzer VM, FortiGuard Indicator of Compromise (IOC) (for 1-6 GB/Day of Logs)	FC1-10-LV0VM-149-02	1	52 888,00-Kč	63 994,48-Kč	52 888,00-Kč	63 994,48-Kč	21%
Podpora, technický a aktualizační servis po dobu 5 let	FortiAnalyzer VM, 24x7 FortiCare (for 1-6 GB/Day of Logs)	FC1-10-LV0VM-248-02	1	64 206,00-Kč	77 689,26-Kč	64 206,00-Kč	77 689,26-Kč	21%
Centrální správa systému pro bezpečnost koncových stanic	je součástí licence pro Bezpečnost koncových stanic		0					

Popis produktu	Název zařízení	Part number	Dodávané množství	Jednotková cena bez DPH	Jednotková cena včetně DPH	Cena celkem bez DPH	Cena celkem včetně DPH	Sazba DPH
Podpora, technický a aktualizační servis po dobu 5 let	je součástí licence pro Bezpečnost koncových stanic		0					
Distribuční síťový přepínač	Catalyst 9200L 24-port PoE+, 4 x 10G, Network Advantage	C9200L-24P-4X-A	4	33 046,00-Kč	39 985,66-Kč	132 184,00-Kč	159 942,64-Kč	21%
Distribuční síťový přepínač	C9200L Cisco DNA Advantage, 24-port	C9200L-DNA-A-24	4	18 910,00-Kč	22 881,10-Kč	75 640,00-Kč	91 524,40-Kč	21%
Distribuční síťový přepínač	Cisco Catalyst 9200L Stack Module	C9200L-STACK-KIT	4	9 800,00-Kč	11 858,00-Kč	39 200,00-Kč	47 432,00-Kč	21%
Záruka, podpora, technický a aktualizační servis po dobu 5 let		Supp-C9200L	4	5 000,00-Kč	6 050,00-Kč	20 000,00-Kč	24 200,00-Kč	21%
SFP moduly pro distribuční síťové přepínače	Cisco GLC-SX-MMD		0					
Záruka po dobu 5 let	je součástí zařízení SFP modulu		0					
Instalace, konfigurace, doprava (***instalace proběhne ve dni pracovního klidu***)		BS práce	1	144 000,00-Kč	174 240,00-Kč	144 000,00-Kč	174 240,00-Kč	21%
CENA CELKEM						**2 621 398,00-Kč**	**3 171 891,58-Kč**	

Veškeré dodané Zboží je nové, nikdy nepoužité, určené pro trh ČR a v ČR i EU servisovatelné ve standardní servisní síti příslušných výrobců se zárukou v délce nejméně 5 let.

Využití/nahrazení stávajících firewallů zadavatele

Firewally a příslušenství	Počet	Využito kusů	Nahrazeno/doplněno čím (typ)
Fortigate 100E	2	2	
Fortigate 60E	2	2	
Fortigate 60F	1	1	
Fortinet FAP21D	3	0	FAP-C24JE-E
Fortinet FP221B	2	0	FAP-221E-E
FortiAnalyzer virtual appliance	1	1	

Využití/nahrazení stávajících SFP modulů zadavatele

Distribuční síťové přepínače	Počet SFP	Využito kusů	Nahrazeno/doplněno čím (typ)
Cisco GLC-SX-MMD	8x	8	

Příloha č. 2 – Technické parametry dodávaného Zboží

Popis stávající podoby sítě a jejího zabezpečení

V současnosti je oblast bezpečnosti řešena dvojicí hlavních firewallů Cisco ASA 5525 v HA clusteru v budově radnice (hlavní konektivita do internetu s propustností 200 MBit), dvojicí firewallů Fortigate 100E v HA clusteru s UTM licencí v budově Městské policie (zajišťuje záložní konektivitu úřadu do internetu s propustností 100 MBit a současně segmentaci sítě MP s propustností 10x 1 Gbit), firewallem Fortigate 60E v budovách zimního stadionu a plaveckého bazénu a zařízením Fortinet Fortigate 60F v budově sportovní haly. Zadavatel předpokládá nahrazení nejméně firewallů Cisco ASA 5525 novými zařízeními, plnícími funkci hlavních firewallů a odpovídající dále v ZD specifikovaným požadavkům.
Firewall v budově Městské policie je rozdělen na dva virtuální firewally. První firewall zajišťuje směrovaní síťového provozu, druhý firewall poskytuje prostřednictvím explicitní proxy ochranu internetového provozu v oblastech ochrany proti virům a jinému škodlivému kódu, ochranu proti přístupu k vybraným kategoriím webových stránek a DLP monitoringu.
Součástí řešení jsou také 4 kusy zařízení FAP21D, které slouží jako příležitostná mobilní pracoviště s metalickým a WiFi připojením, umístěná mimo vnitřní síť magistrátu (zařízení FAP21D jsou připojena k firewallu Fortigate 100E IPSec tunelem).
Pro zajištění provozu vozidla dohledu parkovacích zón jsou v řešení zakomponována dále 2 zařízení Fortinet FP221B, která vozidlu poskytují WiFi konektivitu v prostorách budovy městské policie a Dopravního podniku. Podmínkou pro provoz této sítě je oddělená konektivita AP od vnitřní sítě magistrátu s CAPWAP protokolem a IPSec šifrováním provozu.
Management platformou pro toto řešení je virtuální appliance FortiAnalyzer, která zajišťuje shromažďování a vyhodnocování logů všech komponent řešení (2GB/den).

Seznam stávajících zařízení zadavatele

Typ zařízení	Umístění	Způsob využití	Podpora platná do
Cisco ASA 5525	Radnice	• node HA clusteru • hlavní konektivita do internetu • DMZ zóna s publikací služeb do internetu • VPN koncentrátor Site-to-site • VPN koncentrátor Klient-to-site	
Cisco ASA 5525	Radnice	• node HA clusteru • hlavní konektivita do internetu • DMZ zóna s publikací služeb do internetu • VPN koncentrátor Site-to-site • VPN koncentrátor Klient-to-site	
Fortigate 100E UTM licence	Městská policie	• node HA clusteru • záložní konektivita do internetu • DMZ zóna s publikací služeb do internetu • VPN koncentrátor Site-to-site • VPN koncentrátor Klient-to-site • Konektivita do sítí třetích stran (PČR, HZS, O2, ČD Telematika cloud ..) • Segmentace LAN • Konektivita pro vzdálené lokality zimní stadion, plavecký bazén, sportovní hala, dopravní podnik • WiFi controller pro AP projektu CIS, mobilní pracoviště a sportovní halu • Explicitní proxy server	22.7.2020
Fortigate 100E	Městská	• node HA clusteru	22.7.2020

UTM licence	policie	• záložní konektivita do internetu • DMZ zóna s publikací služeb do internetu • VPN koncentrátor Site-to-site • VPN koncentrátor Klient-to-site • Konektivita do sítí třetích stran (PČR, HZS, O2, ČDTelematika cloud ..) • Segmentace LAN • Konektivita pro vzdálené lokality zimní stadion, plavecký bazén, sportovní hala, dopravní podnik • WiFi controller pro AP projektu CIS, mobilní pracoviště a sportovní halu • Explicitní proxy server	
Fortigate 60E	Zimní stadion	• Firewall zajišťující konektivitu lokality do sítě magistrátu • Segmentace LAN • DHCP server	10.9.2020
Fortigate 60E	Plavecký bazén	• Firewall zajišťující konektivitu lokality do sítě magistrátu • Segmentace LAN • DHCP server	5.9.2020
Fortigate 60F	Sportovní hala	• Firewall zajišťující konektivitu lokality do sítě magistrátu • Segmentace LAN • DHCP server	17.5.2020
Fortinet FAP21D	Mobilní pracoviště	• Konektivita do internetu s dynamickou IP adresou. • Firewall zajišťující konektivitu do sítě magistrátu zabezpečenou CAPWAP protokolem s IPSec šifrováním provozu • WiFi access point • Více SSID zakončených na samostatném interface firewallu Městské policie	20.6.2019
Fortinet FAP21D	Mobilní pracoviště	• Konektivita do internetu s dynamickou IP adresou. • Firewall zajišťující konektivitu do sítě magistrátu zabezpečenou CAPWAP protokolem s IPSec šifrováním provozu • WiFi access point • Více SSID zakončených na samostatném interface firewallu Městské policie	20.6.2019
Fortinet FAP21D	Mobilní pracoviště	• Konektivita do internetu s dynamickou IP adresou. • Firewall zajišťující konektivitu do sítě magistrátu zabezpečenou CAPWAP protokolem s IPSec šifrováním provozu • WiFi access point • Více SSID zakončených na samostatném interface firewallu Městské policie	20.6.2019
Fortinet FP221B	Městská policie	• AP s konektivitou k firewallu Městské policie zabezpečenou CAPWAP protokolem s IPSec šifrováním provozu • WiFi access point • Více SSID zakončených na samostatném interface firewallu Městské policie	20.6.2019
Fortinet FP221B	Dopravní podnik	• AP s konektivitou k firewallu Městské policie zabezpečenou CAPWAP protokolem s IPSec	20.6.2019

		šifrováním provozu • WiFi access point • Více SSID zakončených na samostatném interface firewallu Městské policie	
FortiAnalyzer virtual appliance	VMware cluster magistrátu	• Sběr logů • Vyhodnocování provozu • Vyhodnocování rizik • Automatická reakce na vzniklé hrozby • Alerting • Reporting • NOC/SOC dashboard pro administrátory • Vizualizace sítě a síťových hrozeb	bez omezení

Pro realizaci předmětu zakázky je možné využít i v tabulce uvedená stávající zařízení, která jsou již v majetku Zadavatele. Při zachování stávajících komponent musí být součástí dodávky zajištění podpory a rozšíření licencí (pro splnění požadavků ZD) na období nejméně 5 let od data předání a převzetí předmětu plnění.

Cíle projektu

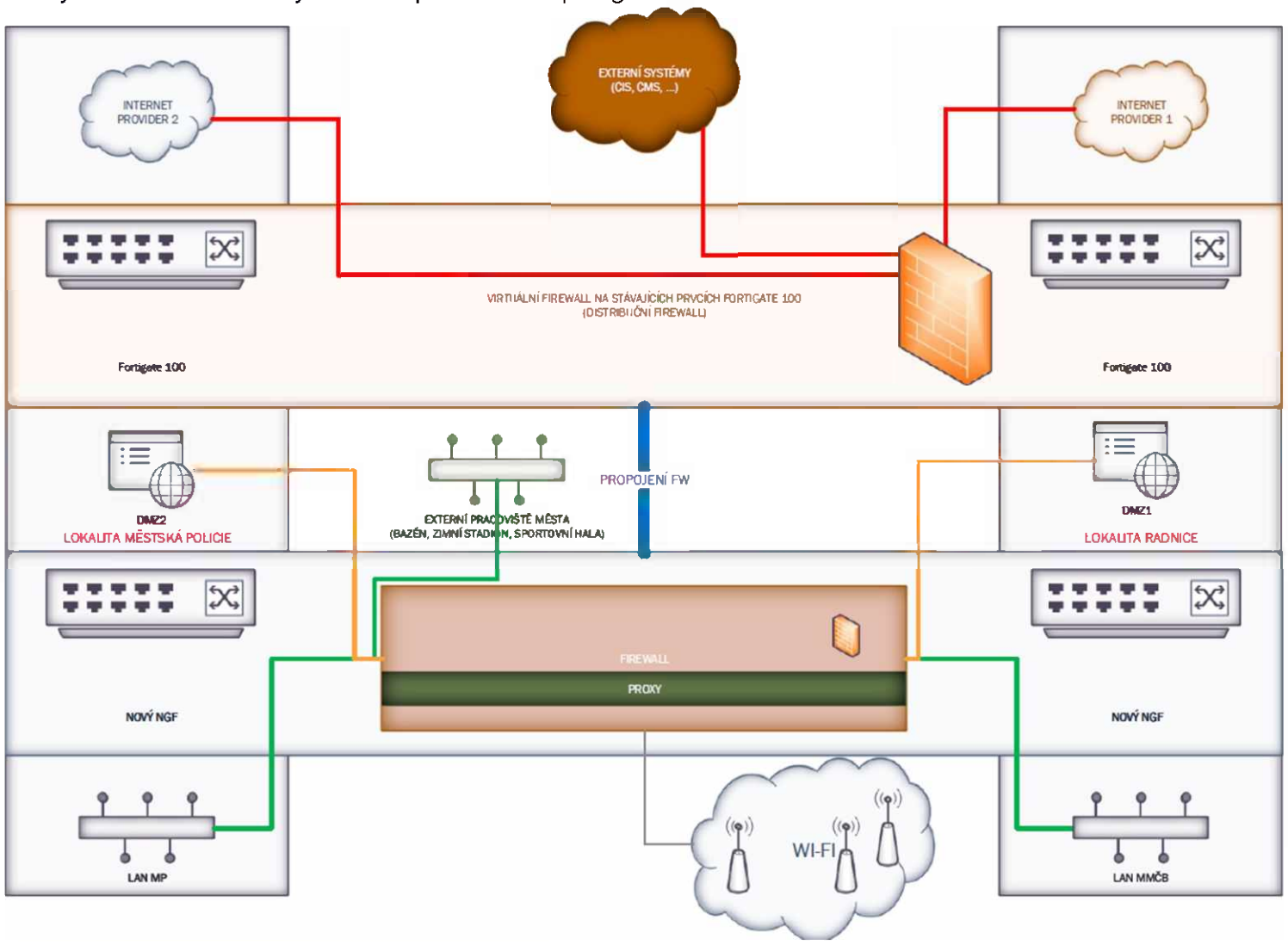
Cílem projektu je dodávka zařízení včetně podpory a implementace, které rozšíří nebo nahradí stávající řešení při splnění všech požadavků této ZD. Všechna zařízení dodaná v rámci této zakázky musí být nová, nikde nepoužitá, se zajištěnou podporou v ČR, určená pro trh ČR.

Modernizace stávajícího řešení je požadována především v následujících oblastech:

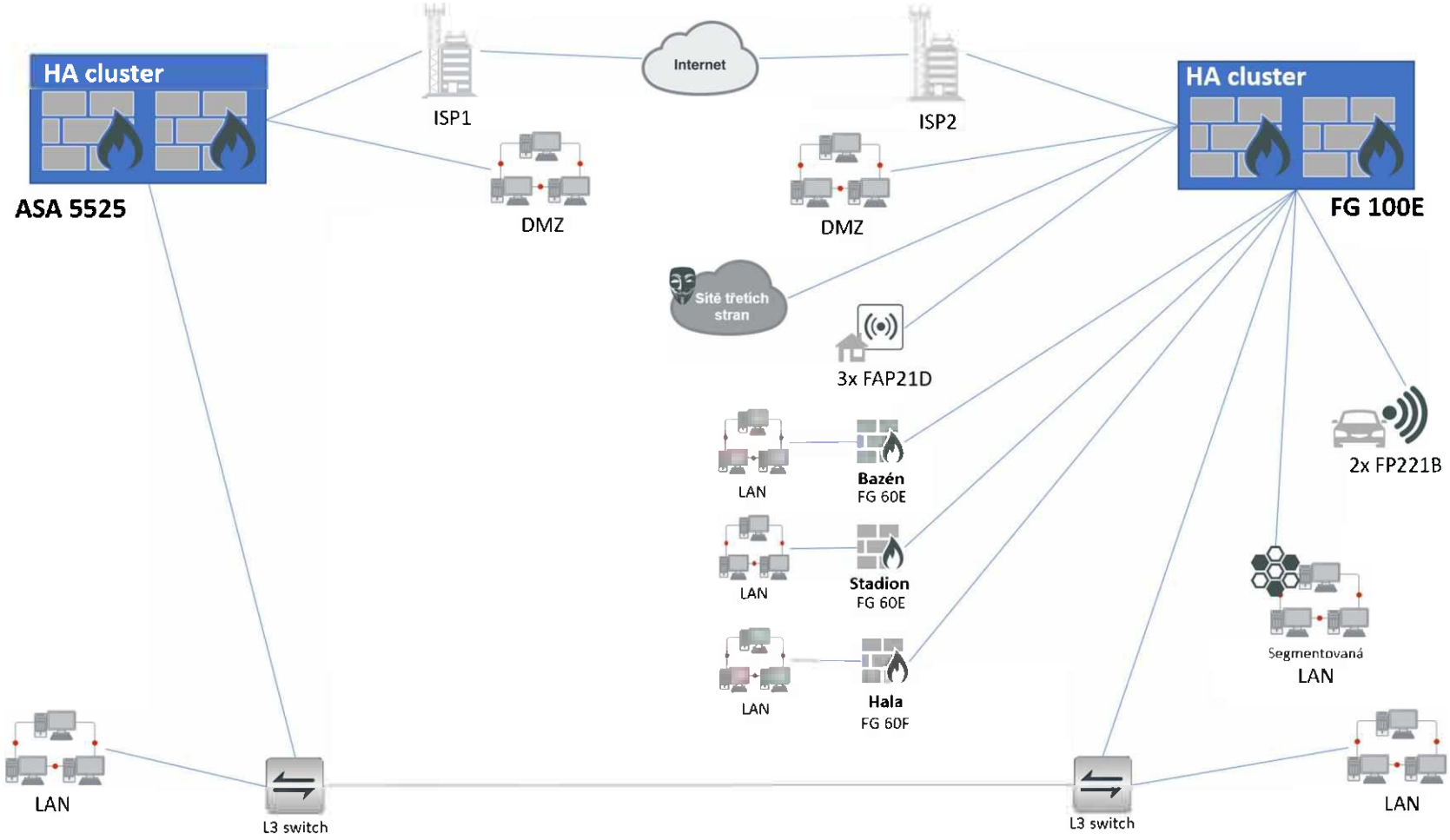
- Náhrada stávajících firewallů Cisco ASA5525 tzv. next generation firewally. Zadavatel nevylučuje ani možnost náhrady dalších firewallů a SW nástrojů dle uvážení účastníka tak, aby bylo dosaženo požadované funkcionality
- V případě zachování části již užívaných firewallů a SW nástrojů i v případě dodávky nových produktů musí být součástí nabídky i zajištění SW a HW podpory všech těchto zařízení na 5leté období, vyjma Fortinet FAP21D a Fortinet FP221B
- Správa všech zařízení (nově dodaných i případně ponechaných stávajících) musí probíhat jednotně přes společné konfigurační rozhraní
- Segmentace interní sítě LAN
- Zajištění vysoké dostupnosti přístupu celého úřadu na internet s odolností proti výpadku zařízení nebo hlavní či záložní konektivity do internetu
- Vysoká dostupnost segmentačního firewallu s odolností proti výpadku celé lokality pro vybrané VLAN
- Funkce Link Load Balancing, která dokáže řídit komunikaci do a z internetu na základě vybraného typu komunikace a umožní kapacitně vytížit obě stávající používaná internetová připojení
- Automatické ověřovaní síťového provozu na základě přihlášeného uživatele včetně prostředí RDP serverů Microsoft Windows, bez nutnosti interaktivního ověřování uživatelů
- Možnost ověřování VPN prostřednictvím vícefaktorové autentizace pro uživatele active directory i pro lokální uživatele firewallu. Realizované řešení musí obsahovat testovací prostředí na neomezenou dobu pro omezený počet uživatelů (≥5)
- Možnost ověřování administrátorů firewallu prostřednictvím vícefaktorové autentizace pro uživatele active directory i pro lokální uživatele firewallu. Realizované řešení musí obsahovat testovací prostředí na neomezenou dobu pro omezený počet uživatelů (≥5)
- Posílení stávajícího řešení ochrany internetové komunikace prostřednictvím explicitní proxy s důrazem na následující funkcionality:
    - klasifikace kategorie webových serverů
    - ochrana před botnet CNC servery
    - full SSL inspekce s možností vyloučení na základě statických záznamů a prostřednictvím definovaných kategorií webových serverů
    - antivirová ochrana
    - DLP řešení
    - aplikační ochrana
- IPS ochrana všech segmentů sítě (předpokládáme umístění FW v centru sítě) LAN
- Detekce síťového provozu na základě aplikace a následné řízení provozu na základě kategorie aplikací nebo staticky definovaných aplikací. Možnost vytváření vlastních aplikačních vzorků pro detekci
- Ochrana DNS na základě dynamických kategorií, statických black/white listů a dynamických botnet/malware dotazů
- Detekce a monitoring provozu koncových zařízení ve vybraných sítích
- Automatická blokace zařízení na základě vyhodnocených hrozeb
- Řízený přístup do sítě a VPN podmíněný splněním bezpečnostních podmínek koncových bodů
- Sledování zranitelností operačního systému a aplikací na koncových bodech
- Reverzní proxy pro bezpečné publikování služeb do internetu

- Ochrana firewallu proti DOS útokům s možností konfigurace úrovně ochrany
- QoS s možností definice pravidel na základě:
    - uživatele
    - aplikace/kategorie aplikací
    - zdrojové IP
    - cílové IP
    - internetové služby
    - času
    - možnost definice „per IP“ pravidel
- Centrální sběr a vyhodnocování bezpečnostních záznamů a statistik provozu ze všech komponent řešení s důrazem na následující funkcionality:
    - sběr a uchování záznamů na dobu nejméně 365 dní s možností online vyhledávání a filtrování v reálném čase
    - vyhodnocování síťového provozu
    - vizualizace sítě a síťových hrozeb
    - vyhodnocování rizik včetně zranitelnosti koncových bodů
    - inteligentní korelace bezpečnostních záznamů s následným vyhodnocením nebezpečí na koncových bodech
    - automatická reakce na vzniklé hrozby
    - vytváření podrobných reportů s možností vytváření vlastních šablon
    - odesílání varovných hlášení při výskytu definovaných událostí
    - dashboard pro online sledování hrozeb administrátory systému
    - napojení na stávající systém LogManager
- Ochrana koncových bodů s důrazem na:
    - antivirovou ochranu
    - vyhodnocování a opravu zranitelností operačního systému a aplikací
    - ochranu síťového provozu (personal firewall)
    - ochranu webového provozu
    - centrální management koncových bodů
    - VPN klienta pro připojení do interní sítě pro mobilní zařízení

Následující obrázek znázorňuje schéma plánované topologie sítě.



Následující obrázek znázorňuje schéma stávající topologie řešení



NG Firewall – Distribuční

Požadujeme 2 ks firewallu typu NGFW (New Generation Firewall) zapojené v režimu vysoké dostupnosti dle níže uvedené specifikace. Dodávka musí obsahovat všechny HW komponenty, licence UTM a aktualizační servis na dobu 5 let. Součástí dodávky 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.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
2 x NGFW v podobě HW appliance (ideálně o velikosti 1 RU)	ANO	
Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, pak musí potřebná licence pro obě varianty být součástí dodávky	ANO	
Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné konfigurační rozhraní	ANO	
Každá appliance minimálně 16 x 1 GbE RJ45 síťových portů, z toho minimálně 2xGbE kombinované RJ45/SFP, případně 16 x 1 GbE RJ45 síťových portů + 2xGbE SFP	ANO	
Konzolový port	ANO	
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a nutnosti instalovat klientskou aplikaci	ANO	
Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)	ANO	
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí kabelů)	ANO	
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	
Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety, …) s možností aplikace do bezpečnostní politiky	ANO	
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence musí být součástí dodávky	ANO	
Funkce QoS, traffic shaping	ANO	
Funkce VPN – klientská (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; ssl vpn nebo ipsec vpn), site-to-site ipsec VPN s podporou statického i dynamického routování	ANO	

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce (dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) pracující jako cloudová služba daného výrobce (součástí musí být předplatné takové služby po dobu platnosti podpory řešení, možnost napojení na vlastní sandbox daného výrobce v budoucnu)	ANO	
Funkce rozpoznávání populárních síťových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace (až do celkového počtu min. 2000)	ANO	
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu	ANO	
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	
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.	ANO	
Podpora funkce loadbalancingu s funkcí SSL offload a možností výběru LB metody (min. round robin, váhované rozdělení, výběr dle nejmenšího počtu aktivních spojení) a detekcí stavu serverů ve skupině (health check) na principu HTTP dotazu	ANO	
Funkce SSL inspekce pro kontrolu protokolů s možností whitelistingu	ANO	
Podpora dvoufaktorové autentizace za pomoci HW tokenů i aplikace pro mobilní telefony (Android, iOS) s podporou autentizace administrátorů při přístupu k firewallu a zároveň pro dvoufaktorovou autentizaci uživatelů do VPN. Tato funkce může být integrována do FW, nebo dodána jako samostatné řešení. Při počáteční instalaci požadujeme minimálně 2 testovací tokeny pro přístup administrátorů. V další fázi může být počet rozšířen pro všechny uživatele přistupující přes VPN (tj. pro až 700 uživatelů) – dodávka tokenů pro plošné nasazení není součástí této zakázky.	ANO	
Funkce wireless kontroleru pro centrální správu bezdrátové sítě, možnost spravovat AP přímo z GUI firewallu	ANO	
Podpora automatické karantény WiFi klientů klasifikovaných firewallem jako problematické, a to až do úrovně odpojení od AP	ANO	
Podpora výrobcem dynamicky udržovaného seznamu IP adres veřejných cloudových služeb	ANO	
SPECIFIKACE VÝKONOVÝCH POŽADAVKŮ		
Celková minimální propustnost firewallu pro IPv4 + IPv6 provoz bude nejméně 7 Gbps (měřeno na UDP komunikaci)	ANO	
Při měření na provozu tvořeném mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50% celkové minimální propustnosti	ANO	
Počet současně navázaných spojení firewallu min. 1 800 000, počet nových spojení za sekundu min. 30 000	ANO	
Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 3,5 Gbps	ANO	
Propustnost SSL VPN min. 200 Mbps	ANO	
Propustnost funkce SSL inspekce min 100 Mbps	ANO	
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza	ANO	

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

aplikací) min. 350 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)		
Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 250 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.	ANO	

NG Firewall – Segmentační

Požadujeme dodání vysoce dostupného řešení firewall pro lokality „Radnice“ a „Městská policie“ typu NGFW pro segmentaci interní sítě LAN dle níže uvedené specifikace. Instalované řešení by mělo být odolné proti výpadku celé fyzické lokality. Dodávka musí obsahovat všechny HW komponenty, licence a aktualizační servis na dobu 5 let. Součástí dodávky musí být přímá technická podpora výrobce (zadavatel musí mít přímý kontakt na centrum technické podpory výrobce) na stejnou dobu, a to v režimu minimálně 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.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	Fortinet
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	FG-600E
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600E.pdf
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
2 x NGFW v podobě HW appliance (ideálně o velikosti 1 RU)	ANO	ANO
Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, pak musí potřebná licence pro obě varianty být součástí dodávky	ANO	ANO
Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné konfigurační rozhraní	ANO	ANO
Každá appliance minimálně 16x 1 GbE síťových portů (minimálně 8x SFP a 8x RJ-45)	ANO	ANO
Každá appliance 2x 10 GbE síťových portů	ANO	ANO
Konzolový port	ANO	ANO
Management port (RJ-45)	ANO	ANO
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a nutnosti instalovat klientskou aplikaci	ANO	ANO
Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)	ANO	ANO
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí kabelů)	ANO	ANO
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	ANO
Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety, …) s možností aplikace do bezpečnostní politiky	ANO	ANO
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence musí být součástí dodávky	ANO	ANO
Funkce QoS, traffic shaping	ANO	ANO

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

Funkce VPN – klientská (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; ssl vpn nebo ipsec vpn), site-to-site ipsec VPN s podporou statického i dynamického routování	ANO	ANO
Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce (dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) pracující jako cloudová služba daného výrobce (součástí musí být předplatné takové služby po dobu platnosti podpory řešení, možnost napojení na vlastní sandbox daného výrobce v budoucnu)	ANO	ANO
Funkce rozpoznávání populárních síťových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace (až do celkového počtu min. 2000)	ANO	ANO
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu	ANO	ANO
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	ANO
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.	ANO	ANO
Podpora funkce loadbalancingu s funkcí SSL offload a možností výběru LB metody (min. round robin, váhované rozdělení, výběr dle nejmenšího počtu aktivních spojení) a detekcí stavu serverů ve skupině (health check) na principu HTTP dotazu	ANO	ANO
Funkce automatického auditu vlastní konfigurace firewallu s ohledem na detekci kritických zranitelností, chyb v konfiguraci bezpečnostní politiky a generování série doporučovaných akcí vedoucí k nápravě a posílení úrovně zabezpečení sítě; součástí funkce musí být pravidelná aktualizace auditních pravidel výrobcem	ANO	ANO
Funkce SSL inspekce pro kontrolu protokolů s možností whitelistingu	ANO	ANO
Podpora dvoufaktorové autentizace za pomoci HW tokenů i aplikace pro mobilní telefony (Android, iOS) s podporou autentizace administrátorů při přístupu k firewallu a zároveň pro dvoufaktorovou autentizaci uživatelů do VPN. Tato funkce může být integrována do FW, nebo dodána jako samostatné řešení. Při počáteční instalaci požadujeme minimálně 2 testovací tokeny pro přístup administrátorů. V další fázi může být počet rozšířen pro všechny uživatele přistupující přes VPN (tj. pro až 700 uživatelů) – dodávka tokenů pro plošné nasazení není součástí této zakázky.	ANO	ANO
Funkce wireless kontroleru pro centrální správu bezdrátové sítě, možnost spravovat AP přímo z GUI firewallu	ANO	ANO
Podpora automatické karantény WiFi klientů klasifikovaných firewallem jako problematické, a to až do úrovně odpojení od AP	ANO	ANO
Podpora výrobcem dynamicky udržovaného seznamu IP adres veřejných cloudových služeb	ANO	ANO
SPECIFIKACE VÝKONOVÝCH POŽADAVKŮ		
Celková minimální propustnost firewallu pro IPv4 + IPv6 provoz bude nejméně 35 Gbps (měřeno na UDP komunikaci)	ANO	ANO

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

Při měření na provozu tvořeném mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50% celkové minimální propustnosti	ANO	ANO
Počet současně navázaných spojení firewallu min. 7 000 000, počet nových spojení za sekundu min. 250 000	ANO	ANO
Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 18 Gbps	ANO	ANO
Propustnost SSL VPN min. 4,5 Gbps	ANO	ANO
Propustnost funkce SSL inspekce min 5 Gbps	ANO	ANO
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	ANO
Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 4,5 Gbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	ANO
Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.	ANO	ANO

NG Firewall pro lokalitu Zimní stadion

Zadavatel umožňuje ponechat stávající technické řešení NGFW a doplnit jej podporami a servisem v požadovaném rozsahu, nebo jej nahradit novým řešením firewallu typu NGFW pro lokalitu „Zimní stadion“ (jinde v textu a obrazové dokumentaci též jen „Stadion“) dle níže uvedené specifikace. V obou případech musí být řešení NGFW zahrnuto pod jednotný management. Dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Součástí dodávky 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 nově 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.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
Minimálně 10x 1 GbE RJ45 síťových portů	ANO	
Konzolový port	ANO	
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a nutnosti instalovat klientskou aplikaci	ANO	
Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)	ANO	
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí kabelů)	ANO	
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	
Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety,…) s možností aplikace do bezpečnostní politiky	ANO	
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence musí být součástí dodávky	ANO	
Funkce QoS, traffic shaping	ANO	
Funkce VPN – klientská (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; ssl vpn nebo ipsec vpn), site-to-site ipsec VPN s podporou statického i dynamického routování	ANO	
Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce	ANO	

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

(dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) pracující jako cloudová služba daného výrobce (součástí musí být předplatné takové služby po dobu platnosti podpory řešení, možnost napojení na vlastní sandbox daného výrobce v budoucnu)		
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 2000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO	
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu	ANO	
Funkce ochrany před síťovými 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	
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.	ANO	
Podpora funkce loadbalancingu s funkcí SSL offload a možností výběru LB metody (min. round robin, váhované rozdělení, výběr dle nejmenšího počtu aktivních spojení) a detekcí stavu serverů ve skupině (health check) na principu HTTP dotazu	ANO	
Funkce SSL inspekce pro kontrolu protokolů s možností whitelistingu	ANO	
Funkce wireless kontroleru pro centrální správu bezdrátové sítě, možnost spravovat AP přímo z GUI firewallu.	ANO	
Podpora automatické karantény klientů klasifikovaných firewallem jako problematické, a to až do úrovně odpojení od AP	ANO	
Podpora výrobcem dynamicky udržovaného seznamu IP adres veřejných cloudových služeb	ANO	
SPECIFIKACE VÝKONOVÝCH POŽADAVKŮ		
Minimální propustnost firewallu pro IPv4 i IPv6 provoz je 3 Gbps (měřeno na UDP komunikaci).	ANO	
Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50%	ANO	
Počet současně navázaných spojení firewallu min. 1 300 000, počet nových spojení za sekundu min. 30 000	ANO	
Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 2 Gbps	ANO	
Propustnost SSL VPN min. 150 Mbps	ANO	
Propustnost funkce SSL inspekce min 135 Mbps	ANO	
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 250 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 200 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.	ANO	

NG Firewall pro lokalitu Bazén

Zadavatel umožňuje ponechat stávající technické řešení NGFW a doplnit jej podporami a servisem v požadovaném rozsahu, nebo jej nahradit novým řešením firewallu typu NGFW pro lokalitu „Bazén“ dle níže uvedené specifikace. V obou případech musí být řešení NGFW zahrnuto pod jednotný management. Dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Součástí dodávky 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 nově 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.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
Minimálně 10x 1 GbE RJ45 síťových portů	ANO	
Konzolový port	ANO	
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a nutnosti instalovat klientskou aplikaci	ANO	
Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)	ANO	
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí kabelů)	ANO	
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	
Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety,…) s možností aplikace do bezpečnostní politiky	ANO	
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence musí být součástí dodávky	ANO	
Funkce QoS, traffic shaping	ANO	
Funkce VPN – klientská (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; ssl vpn nebo ipsec vpn), site-to-site ipsec VPN s podporou statického i dynamického routování	ANO	
Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby);	ANO	

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

podpora sandboxovací funkce (dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) pracující jako cloudová služba daného výrobce (součástí musí být předplatné takové služby po dobu platnosti podpory řešení, možnost napojení na vlastní sandbox daného výrobce v budoucnu)		
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 2000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO	
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu	ANO	
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	
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.	ANO	
Podpora funkce loadbalancingu s funkcí SSL offload a možností výběru LB metody (min. round robin, váhované rozdělení, výběr dle nejmenšího počtu aktivních spojení) a detekcí stavu serverů ve skupině (health check) na principu HTTP dotazu	ANO	
Funkce SSL inspekce pro kontrolu protokolů s možností whitelistingu	ANO	
Funkce wireless kontroleru pro centrální správu bezdrátové sítě, možnost spravovat AP přímo z GUI firewallu.	ANO	
Podpora automatické karantény klientů klasifikovaných firewallem jako problematické, a to až do úrovně odpojení od AP	ANO	
Podpora výrobcem dynamicky udržovaného seznamu IP adres veřejných cloudových služeb	ANO	
SPECIFIKACE VÝKONOVÝCH POŽADAVKŮ		
Minimální propustnost firewallu pro IPv4 i IPv6 provoz je 3 Gbps (měřeno na UDP komunikaci).	ANO	
Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50%	ANO	
Počet současně navázaných spojení firewallu min. 1 300 000, počet nových spojení za sekundu min. 30 000	ANO	
Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 2 Gbps	ANO	
Propustnost SSL VPN min. 150 Mbps	ANO	
Propustnost funkce SSL inspekce min 135 Mbps	ANO	
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 250 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 200 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.	ANO	

NG Firewall pro lokalitu Sportovní Hala

Zadavatel umožňuje ponechat stávající technické řešení NGFW a doplnit jej podporami a servisem v požadovaném rozsahu, nebo jej nahradit novým řešením firewallu typu NGFW pro lokalitu „Sportovní hala“ (jinde v textu a obrazové dokumentaci též jen „Hala“) dle níže uvedené specifikace. V obou případech musí být řešení NGFW zahrnuto pod jednotný management. Dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Součástí dodávky 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 nově 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.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
Minimálně 10x 1 GbE RJ45 síťových portů	ANO	
Konzolový port	ANO	
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a nutnosti instalovat klientskou aplikaci	ANO	
Podpora virtuálních kontextů (min. 10 v ceně nabídky), každý z virtuálních kontextů může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí)	ANO	
Virtuální kontexty musí být možné propojit pomocí virtuálních propojů (bez nutnosti propojovat pomocí kabelů)	ANO	
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	
Funkce rozpoznání typu a druhu koncového zařízení (Windows OS, Linux OS, Mac OS, iOS, Android, mobilní zařízení, tablety,…) s možností aplikace do bezpečnostní politiky	ANO	
Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, licence musí být součástí dodávky	ANO	
Funkce QoS, traffic shaping	ANO	
Funkce VPN – klientská (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; ssl vpn nebo ipsec vpn), site-to-site ipsec VPN s podporou statického i dynamického routování	ANO	
Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných office dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora sandboxovací funkce	ANO	

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

(dynamická analýza přenášených souborů na výskyt dosud nepopsaných variant škodlivého kódu) pracující jako cloudová služba daného výrobce (součástí musí být předplatné takové služby po dobu platnosti podpory řešení, možnost napojení na vlastní sandbox daného výrobce v budoucnu)		
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 2000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO	
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu	ANO	
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	
Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě watermarků, popisu regulárním výrazem atp.	ANO	
Podpora funkce loadbalancingu s funkcí SSL offload a možností výběru LB metody (min. round robin, váhované rozdělení, výběr dle nejmenšího počtu aktivních spojení) a detekcí stavu serverů ve skupině (health check) na principu HTTP dotazu	ANO	
Funkce SSL inspekce pro kontrolu protokolů s možností whitelistingu	ANO	
Funkce wireless kontroleru pro centrální správu bezdrátové sítě, možnost spravovat AP přímo z GUI firewallu.	ANO	
Podpora automatické karantény klientů klasifikovaných firewallem jako problematické, a to až do úrovně odpojení od AP	ANO	
Podpora výrobcem dynamicky udržovaného seznamu IP adres veřejných cloudových služeb	ANO	
SPECIFIKACE VÝKONOVÝCH POŽADAVKŮ		
Minimální propustnost firewallu pro IPv4 i IPv6 provoz je 3 Gbps (měřeno na UDP komunikaci).	ANO	
Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50%	ANO	
Počet současně navázaných spojení firewallu min. 1 300 000, počet nových spojení za sekundu min. 30 000	ANO	
Celková propustnost IPSEC VPN při použití AES256-SHA256 min. 2 Gbps	ANO	
Propustnost SSL VPN min. 150 Mbps	ANO	
Propustnost funkce SSL inspekce min 135 Mbps	ANO	
Propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) min. 250 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) min. 200 Mbps (reálná hodnota, měřeno na běžném provozu – real world traffic)	ANO	
Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání. Zadavatel si vyhrazuje právo na otestování výkonových parametrů.	ANO	

Konektivita sítě pro projekt CIS

WIFI AP pro zajištění provozu vozidla dohledu parkovacích zón, která vozidlu poskytují WiFi konektivitu v prostorách budovy městské policie a Dopravního podniku. Zadavatel umožňuje ponechat stávající technické řešení WIFI AP a doplnit jej podporami a servisem v požadovaném rozsahu, nebo jej nahradit novým řešením WIFI AP dle níže uvedené specifikace. V obou případech musí být Access pointy řízeny společným managementem integrovaným do dodaného NGFW řešení a prezentovat shodná SSID poskytující konektivitu zakončenou na samostatných síťových rozhraních dodaného firewallu. Podmínkou pro provoz této sítě je oddělená konektivita pro AP od vnitřní sítě magistrátu. Komunikace s centrálním managementem musí být prostřednictvím CAPWAP tunelu s IPSec šifrováním provozu.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	Fortinet
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	FAP-221E-E
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
Provedení Indoor	ANO	ANO
Počet vysílačů 2	ANO	ANO
Minimální počet interních antén 4	ANO	ANO
Frekvenční pásma 2.400 - 2.4835, 5.150 - 5.250, 5.250 - 5.350, 5.470 - 5.725, 5.725 - 5.850	ANO	ANO
Frekvence vysílačů 2.4 GHz b/g/n , 5 GHz a/n	ANO	ANO
Ethernet rozhraní 1 x 10/100/1000	ANO	ANO
Power over Ethernet (PoE), IEEE 802.3af	ANO	ANO
Minimální počet SSID pro klientský přístup 14	ANO	ANO
Způsoby ověřování WPA™ and WPA2™ with 802.1x or Preshared key, WEP and Web Captive Portal, MAC blacklist & whitelist	ANO	ANO
EAP ověřování EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/ EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	ANO	ANO
Tx Power 17dBm	ANO	ANO
IEEE standard 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1X, 802.3af	ANO	ANO

Konektivita sítě pro mobilní pracoviště

Aktivní prvek zajišťující konektivitu mobilního pracoviště do sítě magistrátu. Zařízení musí poskytnout konektivitu pro připojená zařízení, zakončenou na samostatných síťových rozhraní firewallu pro lokalitu Radnice. Připojení aktivního prvku k firewallu magistrátu bude zajišťováno prostřednictvím internetové konektivity v místě aktuálního použití zařízení. Předpokládá se, že předávací rozhraní bude tvořeno ethernetovou konektivitou s dynamicky přidělovanou IP adresou. Zařízení se připojí automaticky bez nutnosti administrátorského zásahu. Přenos dat musí být šifrován prostřednictvím IPSec. Zařízení musí poskytovat ethernetovou a WiFi konektivitu. Zadavatel umožňuje ponechat stávající technické řešení, nebo jej nahradit novým řešením WIFI AP dle níže uvedené specifikace.

Vyplnit pouze v případě, kdy je stávající technické řešení Zadavatele nahrazováno novým zařízením

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	Fortinet
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	FAP-C24JE
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf
SPECIFIKACE FUNKČNÍCH POŽADAVKŮ		
Provedení Indoor	ANO	ANO
Síťová propustnost 300 Mbps	ANO	ANO
Ethernetová konektivita 2x FE RJ45 ports (1x WAN port, 1x LAN port)	ANO	ANO
Počet vysílačů 1	ANO	ANO, 2
Minimální počet interních antén 2	ANO	ANO, 4
Frekvenční pásmo 2.400 - 2.4835	ANO	ANO
Frekvence vysílačů 2.4 GHz b/g/n	ANO	ANO
Minimální počet SSID pro klientský přístup 7	ANO	ANO, 8
Způsoby ověřování WPA™ and WPA2™ with 802.1x or Preshared key, WEP and Web Captive Portal, MAC blacklist & whitelist	ANO	ANO
EAP ověřování EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST	ANO	ANO
IEEE standard 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.1x	ANO	ANO
Tx Power 17dBm	ANO	ANO, 23dBm

Centrální management platforma pro správu všech firewallů v síti

Požadujeme dodání centrální management platformu pro správu všech firewallů v síti. Hlavním cílem pro implementaci systému centrálního managementu je možnost udržovat jednotnou politiku včetně databáze všech objektů a možnost její snadné implementace na všechny firewally v síti, a tedy minimalizace lidské chyby při správě bezpečnostních prvků. Součástí dodávky musí být podpora výrobce v režimu minimálně 24x7, a to na dobu min. 5 let (požadujeme přímou podporu výrobce).

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Systém musí být provozován lokálně v síti zadavatele (management pomocí cloudových služeb není akceptovatelný)	ANO	ANO
Virtuální appliance s podporou VMware	ANO	ANO
Grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS)	ANO	ANO
Počet spravovaných zařízení/virtuálních kontextů musí být minimálně v rozsahu všech zařízení, která jsou součástí požadovaného řešení plus dvě zařízení a dále licenčně rozšiřitelný nejméně na trojnásobek požadovaného řešení.	ANO	ANO
Centrální management pro všechny UTM firewally v síti (tj. firewally dodávané v rámci tohoto projektu, stejně jako firewally stávající)	ANO	ANO
Možnost rozdělení zařízení na oddělené administrativní sekce (každý firewall či jeho virtuální kontext může být v jiném administrativním kontextu centrálního logovacího zařízení)	ANO	ANO
Možnost nastavení centrálních politik pro všechna zařízení	ANO	ANO
Podpora RESTful API pro integraci s již aktivními systémy zadavatele	ANO	ANO
Možnost vytváření skupin zařízení na základě jejich geografické polohy nebo logického členění	ANO	ANO
Podpora vytváření vzorů konfigurací pro nově instalovaná zařízení	ANO	ANO
Možnost vytváření a aplikace konfiguračních skriptů pro spravované firewally	ANO	ANO
Revize konfigurací spravovaných firewallů, jestli nejsou pravidla duplikována	ANO	ANO
Ukládání konfiguračních revizí a porovnávání změn mezi nimi	ANO	ANO
Podpora SNMP, logování na SYSLOG server	ANO	ANO
Podpora centrálního upgradu firmwaru spravovaných firewallů	ANO	ANO
Podpora správy licencí spravovaných firewallů	ANO	ANO
Podpora stahování signatur přes centrální management pro spravovaná zařízení	ANO	ANO
Podpora centrální konfigurace a monitoring VPN sítě	ANO	ANO
Možnost správy administrátorských účtů na základě profilů, kde dle přiřazeného profilu bude mít daný administrátor oprávnění vidět nebo spravovat zařízení v různých administrativních kontextech	ANO	ANO
Možnost nastavení módu, kdy bude hlavní administrátor schvalovat změny v konfiguraci firewallů ještě před tím, než se aplikují	ANO	ANO
Podpora vzdáleného ověření administrátorů přes RADIUS a LDAP	ANO	ANO
Podpora vyhledávání v pravidlech, vyhledávání textových výrazů/objektů/IP adres nebo prohledávání všech objektů	ANO	ANO

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

Konzistentní modifikace politiky více administrátory najednou, konzistence politik na základě uzamykání pravidel, politik a objektů	ANO	ANO
Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	ANO	ANO
Integrovaný monitoring musí poskytovat grafické rozhraní pro ledování parametrů v reálném čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd ...).	ANO	ANO
Podpora revizí bezpečnostních politik, jejich verzování	ANO	ANO
Podpora auditních informací u změn bezpečnostní politiky (kdo provedl změnu)	ANO	ANO

Bezpečnost koncových stanic (telemetrie)

Nedílnou součástí bezpečnostní infrastruktury a zároveň jedním z klíčových bodů naší bezpečnostní politiky je zajištění bezpečnosti koncových stanic. V rámci tohoto projektu požadujeme plnou integraci firewallové platformy s koncovými počítači tak, aby firewall dokázal získávat z uživatelských stanic detailní informace o stanici samotné i uživateli. Předpokládáme, že pro splnění tohoto požadavku bude nutné nainstalovat na koncové stanice softwarové agenty. Kromě integrace s firewall platformou by mělo dodané řešení pro ochranu klientských stanic poskytovat i další bezpečnostní funkce, popsané níže. Součástí dodávky musí být přímá podpora výrobce, a to minimálně na dobu 5 let.

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Poskytnutá licence pokrývá minimálně 600 stanic	ANO	ANO
Podpora minimálně těchto operačních systémů (Microsoft Windows 10, 8/8.1, 7, Windows Server 2008 R2/2012/2012 R2/2016; Mac OS X 10.12/10.11)	ANO	ANO
Podpora sdílení telemetrických informací s konzolí centrální správy a síťovým firewallem, a to včetně zobrazení provozních informací o stavu endpointu v konzoli v reálném čase. Vynucení minimální úrovně zabezpečení pracovní stanice (tzv. endpoint compliance modul)	ANO	ANO
Vizualizace stavu pracovní stanice (informace o uživateli, verzi OS, IP/MAC adresách, přirazeném profilu)	ANO	ANO
Propojení s bezpečnostní platformou nabízeného výrobce FW a managementu	ANO	ANO
Endpoint klient musí obsahovat agenta pro integraci s dodávanou FW platformou	ANO	ANO
Informace získané z těchto agentů musí být zobrazovány v GUI firewallu nebo centrálního management nástroje	ANO	ANO
Podpora funkce antivirové/antimalware ochrany včetně ochrany proti pokročilým hrozbám metodou sandboxingu na externí appliance (min. pro MS Windows)	ANO	ANO
Podpora funkce kategorizace webových stránek na základě aktualizované a udržované databáze výrobce/dodavatele	ANO	ANO
Podpora funkce aplikačního firewallu s možností pracovat se síťovými aplikacemi dle kategorií	ANO	ANO
Podpora funkce VPN připojení (SSL a IPSEC) s možností navázat VPN před přihlášením do Windows	ANO	ANO
Podpora funkce detekce zranitelností pracovní stanice (OS a vybraných aplikací) včetně funkce sanace dané vulnerability	ANO	ANO
Možnost propojení s externí platformou pro detekci pokročilých hrozeb (ATP), která pracuje metodou sandboxingu (min. pro MS Windows); zamezení uživatelskému přístupu k testovanému souboru během procesu analýzy	ANO	ANO
Vizualizace logické i fyzické topologie infrastruktury až do úrovně koncové stanice/uživatele	ANO	ANO
Koncová zařízení musí být v management rozhraní graficky zobrazena včetně následujících informací: název zařízení, OS, MAC adresa síťových rozhraní, IP adresa. Možnost vyhledávání konkrétních zařízení nebo uživatel na základě	ANO	ANO

minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno		
Vyhledané zařízení musí být znázorněno v rámci vizualizace síťové topologie včetně všech výše uvedených informací	ANO	ANO
Možnost manuálního nebo automatického vložení zařízení do karantény aplikované na úrovni klienta na základě bezpečnostního incidentu detekovaného na firewall platformě	ANO	ANO
Licence cloudové verze sandboxingu.	ANO	ANO

Systém pro centrální ukládání a korelaci logů z firewallů

Kriticky důležitou součástí projektu je systém pro centrální ukládání a korelaci logů v síti zadavatele. Systém musí být plně kompatibilní se všemi firewall zařízeními, které budou v síti zadavatele produkční po dosažení cílového stavu. Systém musí podporovat analýzu logů nad provozem. **Systém musí být dále schopen poskytovat reporty nad logy ze všech firewallů v síti a informovat správce systému o událostech, hrozbách a trendech, které byly v síti zjištěny, a to formou přehledných grafických reportů.** V případě zjištění hrozby z logů musí být zajištěn automatický mechanismus, jak na danou hrozbu reagovat bez nutnosti zásahu administrátora. Jako součást systému pro centrální ukládání a korelaci logů z firewallů je možné zachovat a rozšířit stávající, Zadavatelem provozovaný, systém FortiAnalyzer.

HLAVNÍ PARAMETRY SYSTÉMU PRO SPRÁVU LOGŮ:		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
virtuální appliance s podporou virtualizačního prostředí VMware	ANO	ANO
grafické konfigurační rozhraní dostupné pomocí webového prohlížeče (HTTPS)	ANO	ANO
kapacita úložiště logů minimálně 3TB a minimální limit pro množství přijatých logů za jeden den 6GB	ANO	ANO
podpora virtuálních síťových rozhraní	ANO	ANO
možnost škálovatelného navýšení kapacity úložiště na základě licence	ANO	ANO
možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma (s možností specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě)	ANO	ANO
napojení na hlavní analyzační nástroj – stávající systém LogManager	ANO	ANO
MULTITENANTNOST		
možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení)	ANO	ANO
každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků	ANO	ANO
LOGOVACÍ FUNKCE		
musí se jednat o centrální logovací prvek pro všechny UTM firewally v síti (tj. firewally dodávané v rámci této zakázky, stejně jako firewally stávající)	ANO	ANO
požadujeme obousměrnou komunikaci mezi firewally a logovací platformou. Tj. logy uložené na centrální logovací platformě musí být dostupné přímo z GUI firewallu, bez nutnosti přistupovat na GUI centrální logovací platformy	ANO	ANO
podpora příjmu a ukládání obecných syslog událostí	ANO	ANO
funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites	ANO	ANO
vizualizace provozu nad všemi firewally	ANO	ANO
možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy (drill-down)	ANO	ANO

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

realtime a historický náhled do logů	ANO	ANO
korelace logů	ANO	ANO
dashboard pro online sledovaní hrozeb v síti	ANO	ANO
podpora prohlížení statistických údajů nad logy	ANO	ANO
možnost automatické reakce na straně firewallu, pokud bylo zjištěno napadení některého systému nebo koncové stanice (zablokování/odpojení)	ANO	ANO
REPORTING		
podpora reportů nad logy ve formátech HTML/CSV/XML/PDF	ANO	ANO
generování reportů v pravidelných nastavitelných intervalech	ANO	ANO
předdefinované vzory pro reporty na nejčastější použití	ANO	ANO
možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze	ANO	ANO
možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky	ANO	ANO
DALŠÍ FUNKCE		
event management – upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou	ANO	ANO
dashboard pro využití dohledovým centrem	ANO	ANO
možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace	ANO	ANO
MOŽNOSTI SPRÁVY A KOMUNIKACE		
podpora SNMPv2, SNMPv3	ANO	ANO
podpora REST API	ANO	ANO
správa přes webové rozhraní HTTPS	ANO	ANO
administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)	ANO	ANO
podpora statického routování	ANO	ANO
možnost zašifrování spojení mezi zařízením které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace	ANO	ANO

Centrální správa systému pro bezpečnost koncových stanic

Systém pro zabezpečení koncových stanic musí být centrálně spravován, pro tyto účely může být dodán samostatný management systém. Součástí dodávky musí být přímá podpora výrobce, a to minimálně na dobu 5 let.

Systém pro centrální správu agentů pro ochranu koncových stanic musí splňovat minimálně následující požadavky:

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Aplikace běžící na MS Windows prostředí (Microsoft Windows Server 2016, 2012, 2012 R2, 2008 R2)	ANO	ANO
Poskytnutá licence pokrývá minimálně 600 instalací klientského software, s možností rozšíření pomocí dokoupené licence	ANO	ANO
Propojení s doménou (Active Directory)	ANO	ANO
Možnost aplikovat různé konfigurační profily na různé organizační složky AD	ANO	ANO
Podpora funkce vzdálené řízené instalace SW na zabezpečení pracovních stanic na předmětné PC v síti	ANO	ANO
Podpora centralizované funkce aktualizace sw na zabezpečení pracovních stanice	ANO	ANO
Podpora funkce centrálního řízení všech zde uvedených bezpečnostních profilů (antivirová inspekce včetně sandboxingu (min. pro MS Windows), kategorizace webových stránek, profily pro připojení do VPN...)	ANO	ANO
Funkce provedení antivirové kontroly vybrané stanice (vybraných stanic) na vyžádání	ANO	ANO
Funkce provedení testu na přítomnost zranitelností vybrané stanice (vybraných stanic) na vyžádání	ANO	ANO
Sběr a definice logů, analýza odhalených incidentů včetně grafické vizualizace	ANO	ANO
Umístění kompromitované stanice do karantény (z pohledu sítové komunikace)	ANO	ANO
Možnost navýšit počet licencí spravovaných endpointů v budoucnu	ANO	ANO

Distribuční síťové přepínače (switche)

Součástí dodávky Zadavatel požaduje dodávku **4 ks distribučních** síťových přepínačů, příslušenství, instalačních a servisních prací v požadovaném rozsahu a ve specifikaci technických podmínek uvedených níže.

SMČB provozuje v rámci města České Budějovice datovou síť LAN zajišťující jednak propojení budov magistrátu a Městské policie ČB s datovými centry, jednak distribuci dat v rámci jednotlivých budov. LAN infrastruktura SMČB je postavena na aktivních prvcích firmy Cisco Systems (cca 100 kusů). Ve všech objektech je provedena strukturovaná kabeláž CAT-5e a vyšší, jako komunikační protokol je použit protokol TCP/IP. Propojení budov je provedeno optickými trasami ve vlastnictví SMČB. Propojení serverovny a patrových rozvaděčů je z větší části rovněž realizováno optickou kabeláží.
Pro dohled a správu stávajícího LAN prostředí je používán balík SW nástrojů pro management sítě Cisco Prime Infrastructure 3.3. doplněný SEM (Security Event Management) systémem LOGmanager ve verzi 3.2.2.

Poptávanými aktivními prvky bude nahrazena část stávající technické infrastruktury Zadavatele. Dodávku je nutné realizovat se zajištěním plné kompatibility se stávající technologií. Tato kompatibilita je nezbytná jak k zajištění plné funkcionality síťové komunikace v síti SMČB, tak i k zajištění kompatibility z pohledu správy služeb a navazujících technických řešení. Kompatibilita je požadována na technické úrovni se stávajícím řešením a rovněž s nástroji pro dohled a správu.

Zadavatel aktuálně využívá v nahrazovaných prvcích následující sadu modulů SFP, které je možno využít v navržených distribučních přepínačích:

Cisco GLC-SX-MMD	8 ks

Zadavatel umožňuje dodavateli v rámci ochrany již dříve zadavatelem realizované investice využít tuto sadu SFP modulů, nebo libovolnou její podmnožinu pro realizaci konektivity nově dodaných zařízení do stávající sítě LAN. Zadavatel nepožaduje, aby dodavatel přebral záruku za tyto stávající SFP moduly zadavatele.
V případě, že dodavatel všechny nebo část těchto modulů nevyužije, musí být nevyužité moduly v rámci dodávky nahrazeny stejně rozsáhlou sadou nových modulů pro připojení ke stávající síťové infrastruktuře zadavatele. Tyto nové moduly musí být stejných nebo lepších vlastností, plně kompatibilní s dodanými zařízeními a se zárukou shodnou s dodanými zařízeními (záruka v délce nejméně 5 let).

Součástí dodávky budou konfigurační služby provedené v rozsahu a za podmínek dle následujícího seznamu:

- Analýza stávajícího prostředí, konfigurací, topologií, záměru zadavatele – v sídle zadavatele
- Návrh konfigurací a postupu implementace– odsouhlasení v sídle zadavatele
- Návrh migračního scénáře – odsouhlasení v sídle zadavatele
- Zahoření dodaných zařízení
- Základní konfigurace a aktualizace přepínačů
- Doprava do lokalit zadavatele
- Instalace do racků (více budov zadavatele v různých lokalitách s max. vzdáleností do 1 km)
- Konfigurace přepínačů v sídle zadavatele
- Migrace topologie sítě bez dopadu na dostupnost síťových služeb (migrace topologie sítě je třeba provádět mimo hlavní pracovní dobu, tj mimo čas 7:30-17:00 v pracovní dny. V případě nutnosti výpadku síťových služeb musí migrace proběhnout v mimopracovní dny)
- Post-implementační podpora a ladění konfigurací

- Předpokládaný rozsah prací je 4 člověkodny – *pouze pro informaci*

Zadavatel požaduje u poptávaných zařízení dodržení minimálních parametrů uvedených v tabulce níže. Parametry uvedené v tabulkách jsou minimální a musí být ve všech případech dodrženy nebo překročeny. Tj. ve všech požadovaných parametrech musí zařízení vykazovat stejné nebo lepší vlastnosti (z pohledu konkrétního technického parametru).

TABULKA POŽADAVKŮ		
Požadovaná funkcionalita/vlastnost	**Akceptovatelná minimální úroveň splnění vlastnosti**	**Způsob splnění požadované funkcionality/vlastnosti (konkrétní hodnota parametru / ANO / NE)**
Výrobce zařízení	Uvedení výrobce	Cisco Systems
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	C9200L-24P-4X-A C9200L-STACK-KIT C9200L-DNA-A-24
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce ***(uvedení odkazu nenahrazuje povinnost přiložení technického listu zařízení k nabídce)***	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html
Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Stohování požadováno	ANO	ANO
Počet dedikovaných stohovacích portů	2	2
Minimální počet zařízení ve stohu	8	8
Minimální kapacita sběrnice stohu	80 Gb/s	80 Gb/s
Stateful Switch Over v rámci stohu - *	ANO	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Redundantní ventilátory	ANO	ANO
Datový stohovací kabel požadován	ANO	ANO
Počet portů 10/100/1000 Base-TX s PoE+ napájením	24	24
Minimální PoE budget	350W	370W
Uplink porty	4x10GE SFP+	4x10GE SFP+
Min. velikost sdíleného systémového bufferu	6 MB	6 MB
Velikost MAC address tabulky	16000	16000
Min. počet IPv4 routes	3000	3000
Min. počet IPv6 routes	1500	1500
Min. počet konfigurovatelných security ACL	1000	1000
IEEE 802.3ad (Link Aggregation)	ANO	ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	48	48

IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	1000
IEEE 802.1x	ANO	ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, web autentizací)	ANO	ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	ANO
RADIUS CoA - *	ANO	ANO
Podpora instance spanning-tree protokolu per VLAN	ANO	ANO
IEEE 802.1w – Rapid Spanning Tree Protocol - *	ANO	ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	ANO
Podpora jumbo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO
OSPFv2	ANO	ANO
OSPFv3	ANO	ANO
ISIS	ANO	ANO
IP Multicast (PIM SSM, PIM SM)	ANO	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
DHCP relay	ANO	ANO
Minimální počet HW QoS front	8	8
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking – DSCP, CoS	ANO	ANO
QoS - Strict Priority Queue	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	ANO
IPv6 QoS	ANO	ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	ANO
IPv6 Port ACL, VLAN ACL	ANO	ANO
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO	ANO
IEEE 802.1ae na uplink portech	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO

Číslo smlouvy kupujícího: **--DOPLNÍ KUPUJÍCÍ--**

Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů - *	ANO	ANO
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	ANO
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	ANO
IEEE 802.3af	ANO	ANO
IEEE 802.3at	ANO	ANO
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače	ANO	ANO
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	ANO
Inteligentní PoE management – zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	ANO
Application Visibility – Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	ANO
Application Visibility – Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	ANO
SSHv2	ANO	ANO
CLI rozhraní	ANO	ANO
Vzdálená identifikace zařízení	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG - *	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO	ANO
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	ANO
SNMPv2/v3	ANO	ANO
Podpora network boot (iPXE)	ANO	ANO
TACACS/+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

*) – zadavatel připouští i jiné, funkčně rovnocenné řešení