KUPNÍ SMLOUVA

(dále jen „smlouva")

uzavřená dle ust. § 2079 a násl. zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „občanský zákoník")

Smluvní strany

Městská část Praha 14

se sídlem:	Bratří Venclíků 1073, Praha 9 – Černý Most
IČO:	00231312
DIČ:	CZ00231312
zastoupená:	Mgr. Radkem Vondrou, starostou
bankovní spojení:	PPF banka, a. s., Praha 6
číslo účtu:	27 – 9800050998/6000
kontaktní osoba:	Ing. Martin Dušek
e-mail / tel.:	[redacted]

(dále jen „kupující")

a

YOUR SYSTEM, spol. s r.o.

zapsán v OR u Městského soudu v Praze, oddíl C, vložka č. 72.

se sídlem:	Türkova 2319/5b, Praha 4, PSČ 149 00
zastoupen:	RNDr. Martinem Nehasilem, jednatelem
IČO:	00174939
DIČ:	CZ00174939
bankovní spojení:	UniCreditBank Česká republika a.s.
číslo účtu:	381610004/2700
kontaktní osoba:	Miroslav Váňa, obchodní ředitel
e-mail / tel.:	[redacted]

(dále jen „prodávající")

(kupující a prodávající společně dále též jako „smluvní strany")

Úvodní ustanovení

Tato kupní smlouva se uzavírá na základě veřejné zakázky „Dodávka firewallové soustavy včetně přepínačů II", která byla realizována jako veřejná zakázka malého rozsahu na dodávky.

I.
Předmět smlouvy

1.1. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu zboží dle technické specifikace uvedené v příloze č. 1 této smlouvy (dále jen „dodávka" či „předmět plnění") a umožnit kupujícímu nabýt vlastnické právo k dodávce, a závazek kupujícího dodávku převzít a zaplatit za dodávku

dále sjednanou kupní cenu. Veškeré dodávané zboží musí být prokazatelně z distribuce určené pro český trh.

1.2 Součástí dodávky je doprava do místa plnění.

II.
Doba a místo plnění

2.1. Prodávající je povinen dodat předmět plnění do dne 31. 12. 2019. Přesný termín dodání prodávající dohodne s kontaktní osobou kupujícího.

2.2. Místem plnění dodávky je sídlo kupujícího.

III.
Kupní cena a platební podmínky

3.1. Kupní cena dodávky je stanovena dohodou a vychází z cenové nabídky prodávajícího v rámci výše uvedené veřejné zakázky příloha č. 2 k této smlouvě:

celková cena bez DPH:	1 176 900,- Kč,
sazba DPH:	21 %
výše DPH:	247 149,- Kč,
celková cena včetně DPH:	1 424 049,- Kč.

3.2. Prodávající vystaví kupujícímu daňový doklad (dále též „faktura") nejdříve ke dni dodání kompletního předmětu plnění. Přílohou této faktury bude kopie předávacího protokolu potvrzeného kupujícím.

3.3. Splatnost faktury činí 15 kalendářních dnů ode dne jejího doručení do sídla kupujícího. Faktura je uhrazena dnem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího, uvedeného v záhlaví této smlouvy.

3.4. Faktura musí obsahovat veškeré náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. V případě, že faktura nebude obsahovat požadované náležitosti, je kupující oprávněn vrátit fakturu zpět prodávajícímu k doplnění, lhůta splatnosti počne běžet znovu od doručení řádně opraveného daňového dokladu.

IV.
Předání a převzetí předmětu plnění

4.1. Prodávající vyzve kupujícího k převzetí předmětu plnění nejpozději 3 pracovní dny přede dnem, kdy bude předmět plnění připraven k předání kupujícímu.

4.2. Kupující je povinen převzít předmět plnění pouze v případě, že předmět plnění bude předáván bez vad a nedodělků.

4.3. Prodávající se zavazuje předat kupujícímu spolu s dodávkou i doklady, které se k jednotlivým součástem dodávky vztahují a jsou potřebné k jejich řádnému užívání.

4.4. O předání a převzetí předmětu plnění sepíší smluvní strany předávací protokol, který bude vyhotoven ve dvou stejnopisech, z nichž jeden obdrží prodávající a jeden kupující.

4.5. Vlastnické právo k předmětu plnění přechází z prodávajícího na kupujícího okamžikem podpisu předávacího protokolu oběma smluvními stranami a předáním předmětu plnění.

V.
Záruka

5.1. Délka záruční doby na dodávku je stanovena v délce 36 měsíců od předání kompletní bezvadné dodávky, s reakcí následující pracovní den.

5.2. Práva z odpovědnosti za vady (reklamace) uplatňuje kupující přímo u prodávajícího písemnou formou.

5.3. Prodávající je povinen odstranit vady, na něž se vztahuje záruka (dále jen „záruční vady"), nejpozději do 10 kalendářních dnů ode dne doručení oznámení kupujícího o vadách, pokud se smluvní strany nedohodnou jinak. Za odstranění záruční vady se považuje stav, kdy je předmět plnění bez této vady předán zpět kupujícímu.

VI.
Sankce

6.1. V případě prodlení prodávajícího s předáním dodávky je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 2.000 Kč za každý započatý den prodlení.

6.2. V případě, že je prodávající v prodlení s odstraněním vady či nedodělku dohodnutého v předávacím protokolu, je povinen zaplatit kupujícímu 500 Kč za každou vadu či nedodělek a za každý den prodlení oproti sjednanému termínu odstranění.

6.3. V případě, že je prodávající v prodlení s odstraněním vady v průběhu záruční doby, je povinen zaplatit kupujícímu 500 Kč za každou vadu a za každý den prodlení oproti termínu uvedeném v odst. 5.3. čl. 5 této smlouvy nebo sjednanému termínu odstranění.

6.4. Zaplacením výše uvedených smluvních pokut není dotčen nárok na náhradu škody.

6.5. Splatnost smluvních pokut činí 30 kalendářních dnů ode dne obdržení písemného vyúčtování.

6.6. Kupující je oprávněn započítat smluvní pokutu proti pohledávce prodávajícího.

VII.
Odstoupení od smlouvy

7.1. Kupující si vyhrazuje právo odstoupit od smlouvy bez jakýchkoli sankcí. Veškeré účelně vynaložené náklady, které budou prokazatelně způsobeny kupujícím a jejichž výše mu bude prodávajícím doložena, budou v takovém případě uhrazeny.

7.2. Odstoupením od smlouvy nejsou dotčena ustanovení této smlouvy týkající se smluvních pokut a těch práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení.

VIII.
Závěrečná ustanovení

8.1. Tato smlouva nabývá platnosti dnem podpisu smluvních stran a účinnosti dnem uveřejnění v registru smluv v souladu s ustanoveními zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.

8.2. Tato smlouva se řídí právním řádem České republiky, zejména občanským zákoníkem.

8.3. Tuto smlouvu lze měnit pouze číslovanými dodatky, podepsanými oběma smluvními stranami.

8.4. Případná neplatnost některého ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení.

8.5. Smluvní strany se dohodly, že případné spory budou přednostně řešeny dohodou. V případě, že nedojde k dohodě smluvních stran, bude spor řešen místně a věcně příslušným soudem.

8.6. Smluvní strany prohlašují, že skutečnosti u vedené v této smlouvě nepovažují za obchodní tajemství ve smyslu občanského zákoníku a udělují souhlas k jejich užití a zveřejnění bez stanovení jakýchkoli dalších podmínek.

8.7. Tato smlouva je vyhotovena v jednom stejnopise v elektronické podobě.

8.8. Smluvní strany prohlašují, že se s obsahem smlouvy řádně seznámily, že byla sepsána dle jejich svobodné a vážné vůle a nebyla sjednána v tísni a za nápadně nevýhodných podmínek.

8.9. Uzavření této smlouvy schválila Rada MČ Praha 14 svým usnesením č. 752/RMČ/2019 ze dne 16. 12. 2019.

Příloha č. 1 - Technická specifikace kupujícího k předmětu plnění včetně
technické specifikace prodávajícího k dodávce

Příloha č. 2 - Položkový rozpočet

V Praze dne [redacted]

[redacted]

.....

kupující
Mgr. Radek Vondra
starosta městské části Praha 14

[redacted]

prodávající
RNDr. Martin Nehasil, jednatel
YOUR SYSTEM, spol. s r.o.

Příloha č. 1

Technická specifikace kupujícího k předmětu plnění včetně technické specifikace prodávajícího k dodávce

A) Technická specifikace kupujícího k předmětu plnění

Předmětem plnění je dodávka bezpečnostní a síťové infrastruktury. Původní zařízení dodavatel bude nadále využívat na svých detašovaných pracovištích během rekonstrukce budov úřadu, a to od 1Q/2020 do 4Q/2022. Dodávka se týká cca. 1/5 aktivní infrastruktury zadavatele. Součástí plnění je mj. dodávka 2 ks centrálních bezpečnostních síťových zařízení a síťových zařízení – tzv. Firewallu, v podobě hardwarového (HW) a softwarového (SW) vybavení, k řízení a zabezpečení síťového provozu mezi interní sítí Zadavatele, internetem a spolupracujícími subjekty, včetně následné tříleté softwarové a servisní podpory od výrobce. Celá dodávka musí obsahovat všechny HW komponenty, licence, záruku a podporu výrobce. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu „end of sales/end of support“. Všechna zařízení/SW musí být určena pro používání v České republice a musí splňovat všechny podmínky stanovené českými normami pro takové používání.
Nabízené řešení musí být 100% kompatibilní se stávající bezpečnostní infrastrukturou, která je tvořena FW Fortinet a síťové prvky HP (HPe) tak, aby bylo možné spravovat všechny provozované zařízení implementovaným administrativním nástrojem v plném rozsahu při zachování stávající pracnosti.
Podrobný popis požadavků je uveden v technické specifikaci „Minimálních požadovaných technických parametrů“.

1. Dodání firewallové soustavy sestávající ze 2 zařízení provozovaných v HA režimu

Dosažitelné parametry
Propustnost FW (1500/512): 18 Gbps
Propustnost FW - (packets per second): 13 Mbps
Propustnost IPS: 2 Gbps
Propustnost IPSec VPN (512 byte): 7Gbps
Propustnost NGFW: 1,5 Gbps
Maximální počet spojení: 2 Mio
Nových spojení za sekundu: 120 000
Musí umožňovat vytvoření HW redundance (clusteru)
Console (RJ-45): 1
15 síťových rozhraní 10/100/1000 Base-T (RJ-45)
velikost max 1U
Požadované podporované funkce
Možnost lokálního uložiště
Podpora virtuálních domén: 10
Podpora mobilních tokenů: (5000)
Podpora všech verzí SSL a TLS (až do verze 1.3 včetně).
Podpora PKI a CLR.
Podpora Client-to-site IPsec VPN.

Podpora Site-to-site IPsec VPN včetně PKI
Stavová synchronizace TCP, UDP a NAT spojení.
Podpora funkce zabezpečení protokolů pro řízení průmyslových technologií včetně rozpoznávání
Plnohodnotná podpora Virtual LAN (VLAN).
Plnohodnotná podpora IPv6 (aplikační vrstva, IPS a dalších bezpečnostních funkcí).
Plnohodnotná podpora Dynamic Host Configuration Protocol (DHCP) relay.
Plnohodnotná podpora Layer 2 (transparent) mode.
Integrace s produkty třetích stran pomocí dokumentovaného API
Vytváření bezpečnostních politik na základě identifikace aplikace na 7 vrstvě OSI modelu
Blokování sítového provozu na základě typu a verze webového prohlížeče, přenášených datových objektů a typu provozu.
Funkce transparentní i explicitní proxy
Podpora řešení je IPS modul včetně ochrany stanic a uživatelů, možnost využít jako sondu pro odhalení nežádoucích aktivit v rámci vnitřní sítě, možnost definice vlastních IPS signatur
Okamžitě použitelné předdefinované IPS politiky.
Antivirový/antimalware engine pro ochranu proti známému škodlivému kódu s možností rozšíření řešení o funkci sandboxingu s API pro integraci s dalšími zdroji
integrovaný nástroje pro analýzu sítě, logování síťového provozu a nástroj pro vytváření cílových reportů ze získaných dat
Mobilní OTP (One Time Password) generátor, el licence: 50

2. Dodání 2 ks páteřních přepínačů

Dosažitelné parametry
I/O porty 10/100/1000 Base-T (RJ-45): 48
SFP+ 10GbE porty: 4
Počet napájených portů PoE: 48
Propustnost (64 byte packets): 190Mpps
Management port (RJ-45):1
USB 2.0: 1
Velikost routovací tabulky IPv4: 4000
Velikost routovací tabulky IPv6: 2000
MAC adres tabulka velikost: 32 000
Paměť: 2GB
Možnost redundantního zdroje
velikost max 1U

3. Dodání 4 ks koncových přepínačů

Dosažitelné parametry
I/O porty 10/100/1000 Base-T (RJ-45): 48
I/O porty 1000/10000 SFP+: 2

Počet napájených portů PoE: 48
Propustnost (64 byte packets): 130Mpps
Management port (RJ-45):1
Velikost routovací tabulky IPv4: 30
Velikost routovací tabulky IPv6: 30
MAC adres tabulka velikost: 16 000
velikost max 1U

4. Dodání 1 ks přepínače pro SAN

Dosažitelné parametry
I/O porty 1000/10000 SFP+: 24
Management port (RJ-45):1
USB 2.0: 1
Velikost routovací tabulky IPv4: 10000
Velikost routovací tabulky IPv6: 5000
Propustnost (64 byte packets): 250Mpps
velikost max 1U
MAC adres tabulka velikost: 64 000
Možnost redundantního zdroje
velikost max 1U

B) Technické specifikace prodávajícího k dodávce

Firewallová soustava sestávající ze 2 zařízení provozovaných v HA režimu **FG-200E** **FortiGate 200E**

Dosažitelné parametry	Splňuje ANO/NE	Jakým způsobem je splněno
Propustnost FW (1500/512): 18 Gbps	ANO	20 Gbps
Propustnost FW - (packets per second): 13 Mpps	ANO	13,5 Mpps
Propustnost IPS: 2 Gbps	ANO	2,2 Gbps
Propustnost IPSec VPN (512 byte): 7Gbps	ANO	7,2 Gbps
Propustnost NGFW: 1,5 Gbps	ANO	1,8 Gbps
Maximální počet spojení: 2 Mio	ANO	2 miliony
Nových spojení za sekundu: 120 000	ANO	135 000
Musí umožňovat vytvoření HW redundance (clusteru)	ANO	
Console (RJ-45): 1	ANO	1
15 síťových rozhraní 10/100/1000 Base-T (RJ-45)	ANO	18
velikost max 1U	ANO	1 RU
Požadované podporované funkce		
Možnost lokálního uložiště	ANO	
Podpora virtuálních domén: 10	ANO	10
Podpora mobilních tokenů: (5000)	ANO	FortiToken 5000
Podpora všech verzí SSL a TLS (až do verze 1.3 včetně).	ANO	
Podpora PKI a CLR.	ANO	

Podpora Client-to-site IPsec VPN.	ANO	
Podpora Site-to-site IPsec VPN včetně PKI	ANO	
Stavová synchronizace TCP, UDP a NAT spojení.	ANO	
Podpora funkce zabezpečení protokolů pro řízení průmyslových technologií včetně rozpoznávání	ANO	
Plnohodnotná podpora Virtual LAN (VLAN).	ANO	
Plnohodnotná podpora IPv6 (aplikační vrstva, IPS a dalších bezpečnostních funkcí).	ANO	
Plnohodnotná podpora Dynamic Host Configuration Protocol (DHCP) relay.	ANO	
Plnohodnotná podpora Layer 2 (transparent) mode.	ANO	
Integrace s produkty třetích stran pomocí dokumentovaného API	ANO	
Vytváření bezpečnostních politik na základě identifikace aplikace na 7 vrstvě OSI modelu	ANO	
Blokování síťového provozu na základě typu a verze webového prohlížeče, přenášených datových objektů a typu provozu.	ANO	
Funkce transparentní i explicitní proxy	ANO	
Podpora řešení je IPS modul včetně ochrany stanic a uživatelů, možnost využít jako sondu pro odhalení nežádoucích aktivit v rámci vnitřní sítě, možnost definice vlastních IPS signatur	ANO	
Okamžitě použitelné předdefinované IPS politiky.	ANO	
Antivirový/antimalware engine pro ochranu proti známému škodlivému kódu s možností rozšíření řešení o funkci sandboxingu s API pro integraci s dalšími zdroji	ANO	
integrovaný nástroje pro analýzu sítě, logování síťového provozu a nástroj pro vytváření cílových reportů ze získaných dat	ANO	FortiAnalyzer
Mobilní OTP (One Time Password) generátor, el licence: 50	ANO	50

Páteřní přepínač - 2 zařízení **JH324A HPE FlexNet 5130 EI 48G**

Dosažitelné parametry	Splňuje ANO/NE	Jakým způsobem je splněno
I/O porty 10/100/1000 Base-T (RJ-45): 48	ANO	48
SFP+ 10GbE porty: 4	ANO	4
Počet napájených portů PoE: 48	ANO	48
Propustnost (64 byte packets): 190Mpps	ANO	190,5 Mpps
Management port (RJ-45):1	ANO	1
USB 2.0: 1	ANO	1
Velikost routovací tabulky IPv4: 4000	ANO	4000
Velikost routovací tabulky IPv6: 2000	ANO	2000
MAC adres tabulka velikost: 32 000	ANO	32768
Paměť: 2GB	ANO	2 GB
Možnost redundantního zdroje	ANO	1
velikost max 1U	ANO	1 RU

Koncový přepínač – 4 zařízení **JG963A** **HPE 1950 48G 2SFP+ 2XGT PoE**

Dosažitelné parametry	Splňuje ANO/NE	Jakým způsobem je splněno
I/O porty 10/100/1000 Base-T (RJ-45): 48	ANO	48
I/O porty 1000/10000 SFP+: 2	ANO	2
Počet napájených portů PoE: 48	ANO	48
Propustnost (64 byte packets): 130Mpps	ANO	130,9 Mpps
Management port (RJ-45):1	ANO	1
Velikost routovací tabulky IPv4: 30	ANO	32
Velikost routovací tabulky IPv6: 30	ANO	32
MAC adres tabulka velikost: 16 000	ANO	16384
velikost max 1U	ANO	1RU

Přepínač pro SAN – 1 zařízení **JL430A** **Aruba 3810M 24SFP+**

Dosažitelné parametry	Splňuje ANO/NE	Jakým způsobem je splněno
I/O porty 1000/10000 SFP+: 24	ANO	24
Management port (RJ-45):1	ANO	1
USB 2.0: 1	ANO	1
Velikost routovací tabulky IPv4: 10000	ANO	10000
Velikost routovací tabulky IPv6: 5000	ANO	5000
Propustnost (64 byte packets): 250Mpps	ANO	285,7 Mpps
velikost max 1U	ANO	1RU
MAC adres tabulka velikost: 64 000	ANO	64000
Možnost redundantního zdroje	ANO	1
velikost max 1U	ANO	1RU

2. ČÁST – VLASTNÍ ROZŠÍŘENÁ TECHNICKÁ SPECIFIKACE ÚČASTNÍKA

Upgrade Firewall a zabezpečení sítě

Upgrade firewallu navrhujeme zachovat stejnou technologii FortiNet, pro aktuální požadavky, a s výhledem na budoucí potřeby úřadu navrhujeme nahradit stávající prvky vyšší řadou FortiGate 200E, s ohledem na vysokou dostupnost v clusterovém řešení, stejně jako jak je stávající řešení.

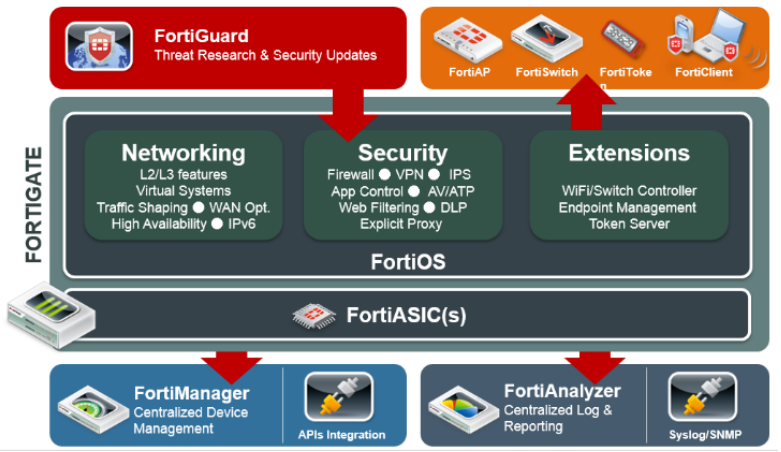
Popis systému FortiGate - Firewall

Platforma FortiGate představuje konsolidované bezpečnostní řešení od společnosti Fortinet. Jedná se o plně hardwarově akcelerované zařízení s vlastním operačním systémem FortiOS. Speciální ASIC procesory jsou určené pro akceleraci funkce firewallu a skenování síťového provozu v reálném čase a umožňují vysoký výkon těchto funkcí nezávisle na velikosti paketu a bez výrazného zatěžování CPU. Kromě síťových a bezpečnostních funkcí platforma FortiGate nabízí ochranu na všech úrovních síťových služeb, jako je kontrola aplikací nezávisle na TCP portu, přístupu na webové stránky, explicitní web proxy, antivirová kontrola, nebo systém IPS. Celé řešení plně podporuje virtualizaci v

rámci daného HW zařízení, což umožňuje rozdělit platformu až na deset plně samostatných a plně oddělených virtuálních firewallů.

Licenční politika společnosti FortiNet Inc. je nezávislá na počtu uživatelů nebo chráněných IP adres. To platí pro všechny funkce, které FortiGate nabízí.

Považujeme za důležité zdůraznit následující vlastnosti:



- HW akcelerace funkce zařízení (není zatěžován hlavní CPU)
- Transparentní licenční politika (nic se nelicencuje na počet uživatelů či IP adress)
- Plná virtualizace, 10 virtuálních strojů v základní ceně zakoupeného HW
- Fortinet drží osm ICSA certifikací, z toho 6 certifikací se týká platformy FortiGate (Firewall-corporate, IPSec VPN, SSL VPN, Network IPS, Anti-virus) - jako jediný výrobce bezpečnostních technologií
- Certifikace administrativy USA (FIPS 140-2, Common Criteria EAL4+)
- Web content filtering - CIPA certifikace, NSS certifikace
- Jednotné uživatelské rozhraní od nejnižších modelových řad až po nejvyšší
- HW akcelerace FW, VPN, IPS a dalších bezpečnostních funkcí (FortiASIC procesory)
- Propustnost FW nezávislá na velikosti paketů – díky technologii FortiASIC
- Silné lokální zastoupení (velká instalovaná báze zařízení, obchodní i technické zastoupení, centrum technické podpory v České republice)
- Široké konfigurační a implementační možnosti – router mód nebo transparentní mód
- Extrémně rychlá reakce na nově odhalené bezpečnostní hrozby (PUSH aktualizace antivirových, IPS a IDS bází)
- Vlastní vývoj všech bezpečnostních funkcí a signaturových balíků
- V rámci maintenance je pokryta jak aktualizace software, tak i záruka na hardware

- **Operační systém FortiOS**

Operační systém FortiOS je proprietární hardened operační systém vyvinutý Fortinetem přímo pro platformu FortiGate. Jedná se o plně hardwarově akcelerovaný firewall, založený na ASIC procesorech. Tyto CPU, jsou vyvinuty a vyráběny přímo společností Fortinet.

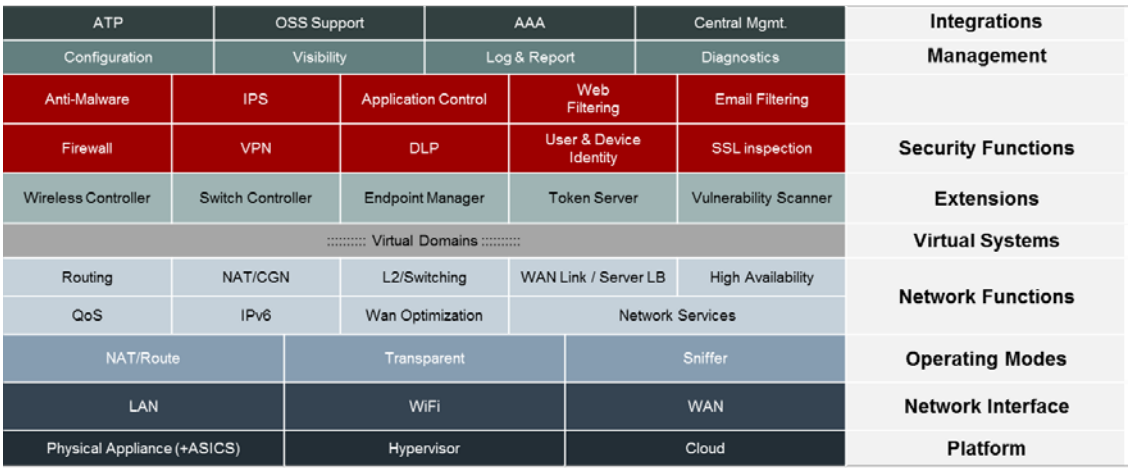
FortiOS nabízí plnou podporu řešením jako je např. VPN, dynamické routování (BGP, OSPF, RIP, Multicast), kompletní logování a audit pro forenzní analýzu, podporu virtualizace Virtual Security Domain (VDOM), aplikační analýzu, antivir a antimalware engine, Sandboxing, IPS s rozšířením pro Web applications firewall, ochranu před mobilním malware, detekcí BYOD zařízení v síti, aplikační kontrolou cloud služeb jako je např. Facebook, Instagram, Twitter, Gmail a mnoho dalších bezpečnostních funkcí a technologií. Nedílnou součástí je také kompletní grafické administrační rozhraní (GUI) dostupné skrze webový prohlížeč, takže odpadá jakákoliv instalace management konzoli na lokální stanici administrátora. Samozřejmostí je i CLI (command line interface - rozhraní s příkazovou řádkou). Neobsahuje žádné komponenty třetí strany, které by mohly mít za následek vznik zranitelností. Splňuje podmínky Common Criteria v úrovni EAL 4+.

Základem produktů z řady FortiGate je pokročilý stavový firewall. Díky své hardwarové architektuře, využití speciálních procesorů typu ASIC a vlastnímu operačnímu systému FortiOS, se

systémy dostávají až na terabitovou propustnost potřebnou pro umístění firewallu uvnitř korporátní sítě (nejvýkonnější rackové řešení se výkonově dostává přes 1Tbps). Díky využité technologii ASIC je výkonnost firewallu prakticky nezávislá na velikosti paketů.

Firewallová pravidla zahrnují kompletní rozsah nastavení pro:

- obousměrnou kontrolu veškerého síťového provozu
- kontrolu šifrovaného provozu ve VPN tunelech
- multiple WAN Link Balancing – připojení k několika různým např. ISP, WAN připojení atd.
- sloučení pravidel a portů do logických skupin
- geo IP filtraci
- aplikování antivirové ochrany
- filtrování obsahu webového provozu
- aplikační analýzu provozu
- detekce IPS/IDS jak protokolové tak aplikační
- blokování a povolování přístupu podle nastavených pravidel
- kontrolu efektivity individuálních pravidel
- povolení nebo odepření přístupu pro individuální adresy, skupiny
- kontrolu standardních a uživatelsky definovaných síťových služeb pro jednotlivce nebo skupiny
- http proxy s možností cache, podpora protokolu WCCPv2, chaining proxy
- SSL dekrypce pomocí Man-in-the-Middle (MiM) mechanizmu
- SSL offloading
- http multiplexing
- vyžádání autentizace uživatele povolením přístupu
- QoS a regulaci šířky pásma včetně možnosti nastavení priority pro každé pravidlo
- NAT/SNAT
- sledování provozu a zápis do logů



- **ASIC® technologie Fortinetu**

Akcelerační prvky FortiASIC představují základ unikátní technologie Fortinetu. Obvody FortiASIC využívají inteligentní a patentovaný engine pro akceleraci funkce firewallu, VPN a skenování obsahu atd., který urychluje činnosti náročné na výpočetní výkon a které v případě běžných firewallových technologií extrémně zatěžují hlavní procesor. Velkou výhodou kromě velkého výkonu je i minimální závislost propustnosti firewallu na velikosti paketů a latence firewallu v řádech jednotek

mikrosekund. Z těchto důvodů je platforma FortiGate extrémně vhodná pro plnění role interního segmentačního firewallu.

Jako další prvek pro zvýšení bezpečnosti informací navrhujeme doplnit celé řešení o FortiAnalyzer, ten v jednom zařízení současně integruje nástroje pro analýzu sítě, logování síťového provozu a nástroj pro vytváření cílových reportů ze získaných dat. Administrátorům sítě přináší hluboký a ucelený přehled o síťovém provozu.

Popis platformy pro analýzu dat - FortiAnalyzer

FortiAnalyzer umožňuje na jednom místě shromažďovat, analyzovat a porovnávat data ze záznamů událostí z distribuované sítě nejen z podnikových firewallů Fortinet, ale i z ostatních zařízení společnost Fortinet a na jednom terminálu zobrazovat veškerý provoz na firewallech a generovat reporty. Při propojení se službou indikátorů narušení FortiGuard (IOC) dokáže poskytovat seznam narušených serverů seřazený podle priorit, což umožňuje rychlou reakci. Zařízení FortiAnalyzer v této architektuře poskytuje podrobný přehled a bezpečnostní výstrahy, na něž lze ihned reagovat nebo s jejich pomocí automatizovat obranu.

Lze jej zakoupit jako HW nebo virtuální appliance.

Hlavní funkce a výhody FortiAnalyzer :

Centralizované vyhledávání a reporting	Jednoduché a intuitivní vyhledávání ve stylu Google a reporty o síťovém provozu, hrozbách, aktivitě a trendech v síti.
Automatizované indikátory narušení (IOC)	Služba FortiGuard IOC vyhledává v bezpečnostních záznamech známky pokročilých perzistentních hrozeb.
Přehled o aktivitě v síti v reálném čase a historické záznamy	Souhrn aplikací, zdrojů, destinací, internetových stránek, bezpečnostních hrozeb, správcovských úprav a systémových událostí.
Základní nástroje pro řízení událostí	Přednastaveným bezpečnostním událostem lze snadno přiřadit automatizované výstrahy.
Hladké zapojení do bezpečnostní architektury Fortinet Security Fabric	Získává informace ze záznamů událostí ze zařízení FortiClient, FortiSandbox, FortiWeb, FortiMail atd. pro dokonalejší přehled.

Přehled funkcí a vlastností

- **FortiView** - podrobný přehled o síti

Přizpůsobitelný interaktivní situační přehled umožňuje rychle identifikovat a řešit problémy

Intuitivní souhrny síťového provozu, hrozeb, aplikací a mnoha dalších informací

Podrobný přehled o uživatelích bezdrátové sítě, cizích přístupových bodech a zranitelnostech koncových zařízení

Vizualizace s bublinovými grafy a geografickou mapou hrozeb

Detailní zkoumání dat umožňuje sledovat stopu útočníka, průběh transakcí a získávat nové poznatky

- **Indikátory narušení FortiGuard** - služba automatizovaného porovnávání dat

Zkoumá bezpečnostní záznamy o provozu ze zařízení FortiGate a vyhledává v nich podezřelé vzorce

Automatizovaný systém obrany proti průniku, který nepřetržitě sleduje známky útoku na síť

Poskytuje podle priority seřazený seznam serverů, u nichž došlo k narušení a je nutné podniknout další kroky

IOC zvyšuje úroveň zabezpečení a pomáhá chránit podnik přesnou a spolehlivou detekcí pokročilých hrozeb

- **Reporting**

Více než 28 předpřipravených šablon připravených k použití se vzorovými reporty

Generování reportů na vyžádání nebo podle harmonogramu s automatickým upozorňováním e-mailem a zobrazením v kalendáři

Flexibilní formáty reportů: HTML/CSV/XML/PDF

Vlastní reporty: přes 300 předdefinovaných grafů pro vlastní reporty a intuitivní nástroj pro tvorbu grafů, který umožňuje snadno vytvářet vlastní grafy z výsledků vyhledávání v záznamech

- **Monitorování a výstrahy**

Aktivní monitorování sítě v reálném čase pro vyhledávání nedostatků, problémů a útoků

Přes 20 předpřipravených definic událostí připravených k použití, s širokými možnostmi vlastních úprav

Automatizované zasílání výstrah umožňuje rychlou reakci

Možnost zkoumání záznamů na velmi podrobné úrovni umožňuje rychlé vyšetření bezpečnostních událostí

- **Multitenantní uspořádání s flexibilním nastavováním kvót**

Nastavitelná časová pravidla pro archivování a analýzu dat pro jednotlivé správcovské domény (ADOM)

Automatizovaná správa kvót podle nastavených pravidel

Grafické zobrazení trendů pomáhá při nastavování pravidel na sledování využití

- **Log Fetch pro forenzní analýzu**

Možnost zpětného vyhledávání v archivovaných záznamech kvůli forenzní analýze z historických dat

Flexibilní možnosti výběru z archivu: vše, nebo pouze vybrané záznamy za určité časové období

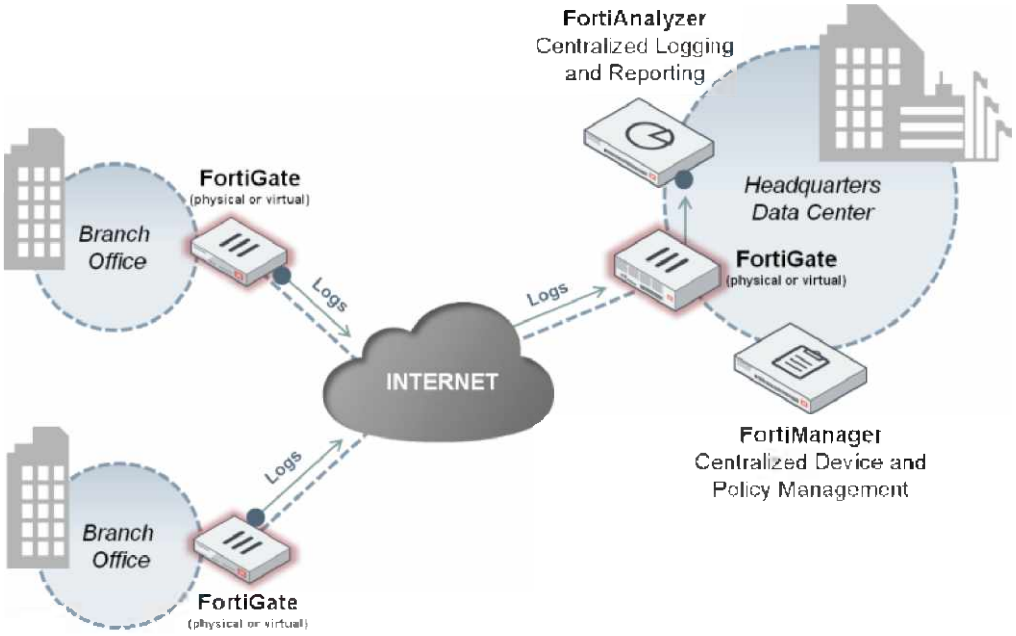
Snadné nastavení vzdáleného získávání archivovaných záznamů ze serveru na několik kliknutí.

- **Předávání záznamů dalším systémům**

Předávání záznamů systémům jako Syslog server, CEF log server nebo FortiAnalyzer pro účely dlouhodobého ukládání, forenzní analýzy nebo jako zákonná povinnost.

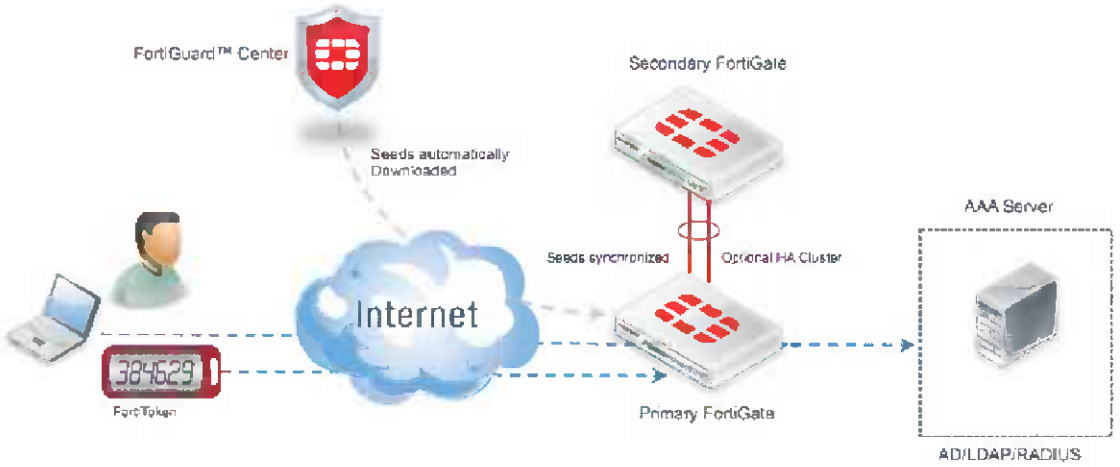
Flexibilní nastavení: předávání všech záznamů nebo pouze vybraných na základě filtrů

Možnost nastavit, která posle záznamu budou předána serverům Syslog nebo CE.



Pro zvýšení bezpečnosti připojení mobilních zařízení do prostředí úřadu navrhujeme použití 100% kompatibilní technologie jakou je FortiToken.

FortiClient nabízí možnost vzdáleného připojení do korporátní sítě pomocí IPSec i SSL VPN. Tato funkce je plně kompatibilní s firewallem FortiGate a nepotřebuje tak žádnou dodatečnou VPN bránu. Nabízí různé možnosti autentizace uživatele jako je dvoufaktorová autentizace včetně využití generátoru jednorázových hesel od Fortinetu (FortiToken).



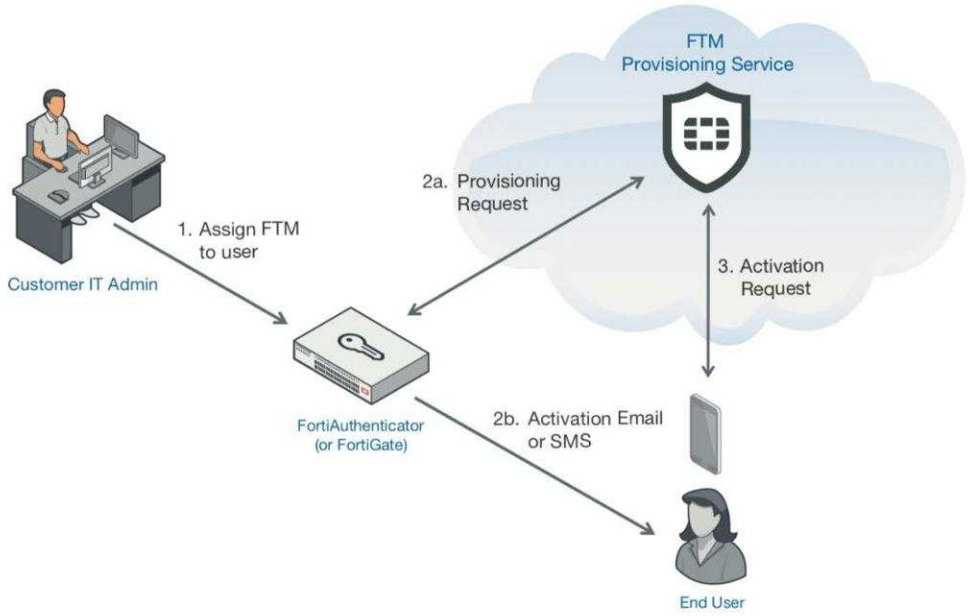
Proces ověření uživatele dvou-faktorovou autentizací pomocí FortiToken vůči FortiGate firewallu autorizační bráně

Dvoufaktorová autentizace

Problematika silných hesel, resp. jejich zapamatování je velmi skloňovaným tématem. Vhodným způsobem řešení silné autentizace uživatelů je přidání druhého faktoru do procesu ověření identity

uživatele, spíše než vynucovaní složitých hesel, které ve svém důsledku vede akorát k tomu, že uživatel si heslo někam zapíše. V rámci dvoufaktorové autentizace uživatel zadává krom svého uživatelského jména a hesla ještě jednorázový kód, který je platný jen omezenou dobu. Kód je uživateli poskytnut různými způsoby. Vždy však platí, že mechanismus poskytnutí jednorázového kódu (tzv. OTP) je pevně spjat se samotným uživatelem. Mezi způsoby, jak uživatel získá jednorázový kód, patří:

- Vygenerování kódu pomocí OTP tokenu – to je přívěšek na klíč s LCD displejem, nebo elektronické zařízení ve tvaru platební karty rovněž s LCD displejem, který po stisknutí tlačítka zobrazí jednorázový kód platný omezenou dobu; OTP token je pomocí sériového čísla asociován s uživatelem
- Vygenerování kódu pomocí mobilní aplikace instalované v mobilním telefonu – uživatel otevře aplikaci (která je chráněna pinem nebo otiskem prstu), vybere si příslušný softwarový token, zobrazené číslo opíše do přihlašovacího dialogu
- Push notifikace – uživatel se přihlašuje do systému, s jeho účtem je svázána tzv. push notifikace, která doručí výzvu na displej uživatelova mobilního telefonu, uživatel odsouhlasí požadavek na přihlášení a spojení se naváže
- Další možnosti (např. doručení kódu s omezenou dobou platnosti pomocí SMS zprávy nebo e-mailové zprávy)



Všechny výše popsané metody mají zásadní vliv na posílení bezpečnosti v souvislosti s ověřováním uživatelů. Případnému útočníkovi již nestačí pro úspěšné narušení systému znát uživatelské jméno a heslo, chybí mu druhý faktor ověření, kterým je jednorázový kód. Tuto funkcionalitu plně podporuje FAC ve spolupráci s ostatními prvky infrastruktury.

Jako náhrada za páteřní přepínač navrhujeme použít technologii HPe, která je již použitá v jiné části infrastruktury. Konkrétně 2x JH324A HPE FlexNetwork 5130 48G 4SFP+ 1-slot HI Switch. Pro rozšíření přípojných portů s rychlostí 10 Gbps 1x JL430A Aruba 3810M 24SFP+ 250W Switch. Náhradu nebo doplnění koncových přepínačů navrhujeme ověřený typ 4x HPe 48G 1950 POE, tento typ už je v infrastruktuře použitý a je spolehlivý.

V Praze dne 17.12. 2019

[redacted]

RNDr. Martin Nehasil, jednatel
YOUR SYSTEM, spol. s r.o.

Příloha č. 2

Položkový rozpočet

	Název	Počet ks	Cena bez DPH za ks	Cena celkem bez DPH
1	Firewallová soustava (2 zařízení)	1	758 400,00 Kč	758 400,00 Kč
2	Páteřní přepínač	2	49 400,00 Kč	98 800,00 Kč
3	Koncový přepínač	4	40 800,00 Kč	163 200,00 Kč
4	Přepínač pro SAN	1	156 500,00 Kč	156 500,00 Kč
	Celkem bez DPH	X	X	**1 176 900,00 Kč**
	Celkem vč. DPH	X	X	**1 424 049,00 Kč**

V Praze, dne 17. 12. 2019

[redacted]

RNDr. Martin Nehasil, jednatel
YOUR SYSTEM, spol. s r.o.