KUPNÍ SMLOUVA č. 19/600/0392

uzavřená podle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, (dále jen „OZ“)

1. Prodávající:

ANECT a.s.
se sídlem: Vídeňská 204/125, Přízřenice, 619 00 Brno

Zastoupená: Janem Zinkem, předsedou představenstva
IČ: 25313029
DIČ: CZ25313029
Bankovní spojeni: Komerční banka, a.s., pobočka Brno
Číslo bank. účtu: [redacted]
(dále jen „prodávající“)

a

2. Kupující:

Česká republika – Generální ředitelství cel
Se sídlem: Budějovická 7, 140 96 Praha 4
Jednající: [redacted]

Spojení: [redacted]

IČ: 71214011
DIČ: CZ71214011
Bankovní spojení: ČNB Praha 1
Číslo účtu: 1020011/0710
Adresa pro doručování korespondence: Budějovická 7, 140 96 Praha 4
(dále jen „kupující“)

Prodávající a kupující společně též označováni jako „smluvní strany“ nebo jednotlivě jako „smluvní strana“.

Prodávající a kupující uzavřeli tuto kupní smlouvu:

I. Předmět plnění

1. Předmětem této kupní smlouvy je dodávka a implementace firewallové soustavy zahrnující dodávku potřebného hardware, licencí, subscripcí a projektových a implementačních prací. Předmět plnění je konkrétně vymezen v příloze č. 1 této kupní smlouvy (Popis předmětu a technická specifikace veřejné zakázky) a dále v příloze č. 2 této kupní smlouvy (Podrobná technická specifikace-tabulka), které jsou nedílnou součástí této smlouvy.

[redacted]

2. Prodávající prohlašuje ve smyslu ust. § 5 OZ, že je odborně způsobilý k zajištění předmětu této smlouvy a po celou dobu trvání závazku bude jednat se znalostí a pečlivostí, která je s touto odborností spojena. Prodávající výslovně prohlašuje, že se seznámil s předmětem smlouvy, dokumentací s ním související a je mu znám i účel, kterého má být touto smlouvou dosaženo.
3. Smluvní strany si výslovně ujednaly, že v případě dodání většího množství předmětu plnění, než je ujednáno v bodu 1 tohoto článku, není kupní smlouva na toto množství uzavřena. Ustanovení § 2093 OZ se tak mezi smluvními stranami neuplatní.
4. Smluvní strany se dohodly, že na vztah založený touto smlouvou se neuplatní § 2126 OZ týkající se svépomocného prodeje, tj. smluvní strany sjednávají, že v případě prodlení jedné strany s převzetím předmětu plnění či s placením za předmět plnění nevzniká druhé smluvní straně právo tuto věc po předchozím upozornění na účet prodlévající strany prodat.

II. Cena a platební podmínky

1. Cena byla stanovena na základě výsledků veřejné zakázky s názvem „Modernizace a rozšíření kapacity firewallových soustav na perimetru sítě CS“ a celkově činí:

   4 953 465,00 Kč bez DPH

   1 040 227,65 Kč 21% DPH

   5 993 692,65 Kč včetně 21% DPH
2. Tato cena byla stanovena jako cena konečná a nelze ji měnit. Cena zahrnuje veškeré náklady včetně nákladů spojených s dopravou, včetně balení podle zvyklostí, do místa plnění.
3. Splatnost řádně vystaveného daňového dokladu – faktury obsahující náležitosti dle příslušných právních předpisů činí 30 dnů ode dne doručení kupujícímu na adresu uvedenou v záhlaví této smlouvy u kupujícího, nebo do datové schránky s následujícími parametry: ID datové schránky „Generální ředitelství cel“: **7puaa4c**
4. Faktura musí obsahovat náležitosti daňového dokladu podle § 435 OZ, podle § 7 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), podle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů a podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a odkaz na tuto smlouvu. Nedílnou přílohou faktur musí být dodací list.
5. Kupující má právo daňový doklad před uplynutím lhůty jeho splatnosti vrátit prodávajícímu, aniž by došlo k prodlení s jeho úhradou, není-li v souladu s příslušnými právními předpisy, nebo není-li přiložen dodací list. Nová lhůta splatnosti v délce 30 dnů počne plynout ode dne doručení opravených daňových dokladů kupujícímu.
6. Peněžní závazek kupujícího se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu prodávajícího. Platba faktur bude provedena bezhotovostním převodem na bankovní účet prodávajícího, jenž je uveden v záhlaví této smlouvy.
7. Platby budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně.
8. Prodávající bere na vědomí, že Kupující je organizační složkou státu, a proto podmínkou financování Kupní ceny bude vydání rozhodnutí „Stanovení výdajů na financování akce organizační složky státu“ v souladu s vyhláškou č. 560/2006 Sb. (o účasti státního rozpočtu na financování programů reprodukce majetku) a pokynu č. R 1 – 2010 (k upřesnění postupu

Ministerstva financí, správců programů a účastníků programu při přípravě, realizaci, financování a vyhodnocování programu nebo akce a k provozování informačního systému programového financování) a s touto skutečností Prodávající výslovně souhlasí. O vydání výše uvedeného rozhodnutí bude Kupující informovat Prodávajícího neprodleně po jeho obdržení. Včasné nezaplacení ceny díla v důsledku této skutečnosti nezakládá prodlení Kupujícího. V případě, že ke dni splatnosti faktury nebude Ministerstvem financí vydáno výše uvedené rozhodnutí, bude o této skutečnosti Prodávající písemně informován Kupujícím. Jakmile bude rozhodnutí vydáno, zašle Kupující Prodávajícímu informaci o této skutečnosti a faktura bude splatná do 10 dnů ode dne doručení této informace Prodávajícímu.

9. Smluvní strany si dojednaly, že kupující je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného správce daně, jestliže se prodávající stane ke dni poskytnutí úplaty za uskutečněné zdanitelné plnění nespolehlivým plátcem daně ve smyslu ust. § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

III. Místo a termín plnění

1. Místem plnění je Generální ředitelství cel, se sídlem Budějovická 7, 140 96 Praha 4, kontaktní osoba [redacted]

2. Pro převzetí předmětu plnění platí, že kupující má právo odmítnout předmět plnění v případě, že podstatným způsobem neodpovídá této smlouvě. Za podstatné se pro účely této smlouvy považuje:

   a) předmětem plnění je množství větší než objednané, v tomto případě má kupující právo odmítnout množství, které přesahuje množství objednané, v případě, že toto šlo při předání jednoduchým způsobem bez použití dalšího zjistit, jinak má lhůtu 5 pracovních dnů na odmítnutí tohoto plnění. Pro splnění této lhůty postačí odmítnutí odeslat,

   b) předmět plnění, který svou jakostí zcela zjevně neodpovídá předmětu plnění kupujícím objednanému,

   c) nedodání kompletní dodávky, např. chybějící doklady k předmětu plnění.

3. Termín dodání předmětu plnění včetně implementace je nejpozději do 6 měsíců od zveřejnění smlouvy v registru smluv. Konkrétní termín dodání hardware bude prodávajícím dojednán min. 24 hod. předem s kontaktní osobou uvedenou v odst. 1 tohoto článku. K dodávce projektových a implementačních prací bude po zveřejnění smlouvy v registru smluv zpracován závazný harmonogram, který bude podepsán zástupci obou smluvních stran.

IV. Podmínky plnění, vlastnické právo

1. Prodávající se touto smlouvou zavazuje dodat kupujícímu předmět plnění a převést na něj vlastnické nebo užívací právo k tomuto předmětu plnění a kupující se zavazuje zaplatit kupní cenu. Kupující nabývá vlastnického nebo užívacího práva k předmětu plnění jeho řádným převzetím na základě podepsaného dodacího listu.

2. Nebezpečí škody na zboží ve smyslu § 2082 odst. 1 OZ přechází na kupujícího okamžikem

převzetí zboží od prodávajícího, tj. na základě podepsaného dodacího listu.

3. Kupující je povinen převzít předmět plnění specifikovaný v článku I. této smlouvy a zaplatit kupní cenu sjednanou v článku II. této smlouvy, s výjimkou ust. čl. III odst. 2.
4. Kupující je povinen poskytnout prodávajícímu, po předchozím sjednání termínu předání podle čl. III odst. 3, součinnost při předání předmětu plnění.
5. Prodávající je povinen zajistit Kupujícímu přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje. Prodávající prohlašuje, že přístup k dokumentaci výrobce zařízení a k průběžně aktualizované znalostní bázi bude funkční nejméně po dobu záruky dle čl. VII. odst. 2 této smlouvy.
6. Prodávající prohlašuje, že Kupující má možnost se zaregistrovat na stránkách výrobce, které Prodávající uvedl ve své nabídce, a které jsou uvedeny v příloze č. 2 této smlouvy v rámci Podrobné technické specifikace dodávaného předmětu plnění, k odběru mailových zpráv týkajících se předmětu dodávky a upozorňujících přinejmenším na:
   - bezpečnostní incidenty, které vyžadují od Kupujícího povýšení operačního systému/firmware či aplikování změny konfigurace či záplaty,
   - konec prodeje či podpory,
   - nové verze operačního systému/firmware
   - známé chyby operačního systému/firmware.

   Prodávající prohlašuje, že služba uvedená v tomto odst. bude funkční nejméně po dobu záruky dle čl. VII. odst. 2 této smlouvy.
7. Prodávající prohlašuje, že Kupující má právo v rámci běhu záruční doby na předmět plnění dle čl. VII. odst. 2 této smlouvy na instalaci obrazu virtuálního serveru výrobce, který bude plnit funkci sondy a bude zajišťovat automaticky funkce uvedené v předchozím odstavci bez nutnosti zpřístupnit zařízení mimo zabezpečenou část sítě.
8. Prodávající prohlašuje, že Kupující je v databázi výrobce veden jako první uživatel zboží (předmětu plnění této smlouvy). Prodávající dále prohlašuje, že všechno dodané zboží, jež je předmětem této smlouvy, je originální a nové.
9. Prodávající se zavazuje doložit Kupujícímu na jeho požádání potvrzení od výrobce o určení dodávaného HW pro evropský trh a Kupujícího jako koncového zákazníka (včetně sériových čísel dodávaných zařízení).
10. Prodávající prohlašuje, že dodávaný předmět plnění, resp. jakékoliv technologie v rámci předmětu plnění (s výjimkou kabelů, spojovacího materiálu) nepochází od výrobců zmíněných v posledních pěti letech publikovaných výročních zprávách BIS v kapitole "Kybernetická bezpečnost" jako zdrojů potenciální hrozby, rizika či jiného nebezpečí na úseku kybernetické bezpečnosti.

V. Smluvní sankce

1. Výslovně se touto smlouvou sjednávají dále stanovené smluvní sankce.
2. Smluvní strany si výslovně ujednaly, že k jiným než zde uvedeným a dále např. ústně sjednaným smluvním sankcím, jakož i k smluvním sankcím sjednaným dodatečně nebude

přihlíženo.

3. V případě, že prodávající nedodrží dodací lhůtu, tak jak je uvedeno v čl. III. odst. 3. této smlouvy, je povinen uhradit kupujícímu smluvní sankci ve výši 3.500,- Kč (slovy: tři tisíce pět set korun českých) za každý započatý den prodlení následující po uplynutí příslušné dodací lhůty.
4. V případě prodlení prodávajícího s odstraněním vady předmětu plnění dle čl. VII. odst. 3 této smlouvy, je prodávající povinen uhradit kupujícímu smluvní sankci ve výši 32.000,- Kč (slovy: třicet dva tisíc korun českých) za každý i započatý den prodlení.
5. V případě prodlení prodávajícího s potvrzením přijetí požadavku (dobou odezvy) dle č. VII. odst. 7 této smlouvy, je prodávající povinen uhradit kupujícímu smluvní sankci ve výši 3.500,- Kč (slovy: tři tisíce pět set korun českých) za každou i započatou hodinu prodlení.
6. Při nedodržení termínu splatnosti faktury, vyjma situace specifikované v čl. II. odst. 8, je prodávající oprávněn požadovat od kupujícího úhradu úroku z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob.
7. Smluvní strany si výslovně ujednaly, že smluvní sankce dle bodů 3, 4 a 5 tohoto článku se nezapočítává na náhradu škody. Dále si smluvní stany výslovně ujednaly, že v případě porušení dle bodu 6 tohoto článku odpovídá výše úroků náhradě škody.
8. Smluvní sankce je splatná do 10 dnů od prokazatelného doručení výzvy k plnění této smluvní sankce.
9. Smluvní strany si vyloučily aplikaci ust. § 1806 OZ, tzn. že úroky z úroků nelze požadovat.

VI. Rozhodné právo a prorogace

1. Vztahy mezi smluvními stranami touto smlouvou výslovně neupravené se budou řídit českými, obecně závaznými právními předpisy, zejména OZ.
2. Smluvní strany podle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů určují jako místně příslušný soud Obvodní soud pro Prahu 1; v případě, že podle procesních předpisů je k rozhodování věci v prvním stupni příslušný krajský soud, určují smluvní strany jako místně příslušný soud Městský soud v Praze.

VII. Záruční podmínky

1. Prodávající výslovně prohlašuje, že dodávaný předmět plnění je bez vad.
2. Prodávající poskytuje na předmět plnění uvedený v čl. I této smlouvy záruku na bezvadnou funkci v délce trvání 36 měsíců. V případě, že bude na faktuře, na dodacím listu nebo na obalu předmětu plnění vyznačena delší záruční doba, má tato přednost před ustanovením této smlouvy. Záruční doba začíná běžet ode dne převzetí předmětu plnění kupujícím.

3. Prodávající se zavazuje po dobu trvání záruky bezplatně odstranit vady předmětu plnění, které se vyskytly po jeho předání, a to v režimu 5x8 NBD, tedy nejpozději během následujícího pracovního dne po nahlášení u závad klasifikovaných jako „Havárie“ – závažná vada zabraňující uživateli využívat základní funkce systému a způsobující nedostupnost dalších služeb navázaných systémů nebo jako „Závada“ – vada zabraňující uživateli využívat rozšířené funkce systému, resp. vada způsobující výrazné snížení užitnosti systému z důvodu degradace výkonu nebo služeb.
4. Prodávající garantuje kompatibilitu konektivitu se stávajícím prostředím včetně požadované úrovně technické podpory během záruční doby. Jakákoliv případná nekompatibilita se stávající infrastrukturou, mající za následek nefunkčnost nebo omezení funkcionality provozovaných zařízení případně komplikace vzniklé ve stávající infrastruktuře v důsledku implementace nově dodaných zařízení musí být řešena prodávajícím na vlastní náklady a může být důvodem k odstoupení od smlouvy.
5. V případě, že nebude možné danou závadu prvku (nebo komponenty) odstranit, bude dodáno náhradní plnění v podobě shodného typu prvku (komponenty).
6. Veškeré náklady související se záruční opravou včetně nákladů spojených s dopravou z míst plnění a zpět hradí prodávající.
7. Prodávající zajistí nepřetržitou Hot-Line pro hlášení servisních požadavků. Tyto požadavky bude možné hlásit elektronicky, nebo telefonicky. Doba odezvy pro potvrzení přijetí požadavku je maximálně 4 hodiny od nahlášení.

[redacted]

VIII. Závěrečná ustanovení

1. Obě smluvní strany se dohodly na tom, že případné dodatky k této smlouvě musí být vyhotoveny pouze písemně, číslované vzestupnou řadou a podepsané oběma smluvními stranami. Smluvní strany si dále ujednaly, že k jiným formám nebude přihlíženo a nebudou jimi vázány.
2. Při podstatném porušení povinností vyplývajících ze smlouvy může každá ze smluvních stran od smlouvy odstoupit. Za podstatné porušení smluvních povinností se považuje nedodržení termínů plnění smluvních stran delší než 30 dnů. Za podstatné porušení smluvních povinností ze strany prodávajícího se rovněž považuje nepravdivost kteréhokoliv prohlášení prodávajícího učiněného v čl. IV. odst. 5, 6, 7, 8 a 10 a dále nesplnění povinnosti prodávajícího uvedené v čl. IV. odst. 5 a 9 a v čl. VII. odst. 4. Toto ovšem neomezuje právo na náhradu škody.
3. Vzájemné vztahy smluvních stran z této smlouvy vyplývající a v ní výslovně neupravené se řídí příslušnými ustanoveními zákona OZ.
4. Tato smlouva se vyhotovuje ve dvou vyhotoveních, z nichž každá strana obdrží jedno vyhotovení.
5. Prodávající výslovně souhlasí s tím, že kupující může tuto smlouvu uveřejnit na svém profilu v plném znění v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

6. Smluvní strany si ujednaly, že závazky vyplývající z této smlouvy se promlčují ve lhůtě 10 (deseti) let ode dne, kdy smluvní strana mohla poprvé toto právo uplatnit.
7. V souladu se zákonem č. 340/2015 Sb., o registru smluv, se strany dohodly, že kupující zašle tuto smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.
8. Smluvní strany si výslovně ujednaly, že tuto smlouvu nelze postoupit na řad. Žádná ze smluvních stran není oprávněna vtělit jakékoliv právo plynoucí jí ze smlouvy nebo z jejího porušení do podoby cenného papíru.
9. Tato smlouva obsahuje následující přílohy:
   Příloha č. 1 – Popis předmětu a technická specifikace veřejné zakázky
   Příloha č. 2 – Podrobná technická specifikace - tabulka

V Praze dne 13. 11. 2019

Jan Zinek

Digitálně podepsal Jan Zinek
Datum: 2019.11.12 17:24:51 +01'00'

.....

Jan Zinek
předseda představenstva

Prodávající

Příloha č. 1 – Popis předmětu a technická specifikace veřejné zakázky

Předmětem výběrového řízení je rozšíření kapacity firewallových soustav na perimetru sítě tak, aby byla navýšena jednak propustnost firewallové soustavy, tak i kapacita současného VPN řešení.

Výchozí stav
Perimetr sítě CS je umístěn ve dvou datových centrech. Primární datové centrum je v centrále GŘC v lokalitě Praha 4, Budějovická a záložní datové centrum je umístěno v datovém centru SPCSS v lokalitě Praha 3, Na Vápence. V každém datovém centru je umístěn jeden firewall klastr složený ze dvou zařízení ASA5545X s Firepower modulem sloužícím jako IPS, Anti-Malware protection a URL filtering. Tyto firewally slouží jako perimetrový firewall, který kontroluje provoz mezi Internetem, DMZ, vnitřní sítí a externími zónami a jedná se o primární bezpečnostní zařízení na perimetru sítě. Dále je v každém datovém centru umístěný jeden firewall klastr složený ze dvou zařízení ASA5515X, sloužící jako VPN koncentrátor. Na VPN koncentrátoru jsou provozovány služby klientských VPN a Site-To-Site VPN.

Požadovaný stav – předmět plnění
Kupující požaduje dodat návrh řešení a potřebný hardware, software a subscripce a provést reimplementaci firewallové soustavy. Řešení bude spočívat v dodávce tří firewallů, které nahradí stávající firewally ASA5545X v roli perimetrových firewallů. Z důvodu zajištění bezproblémové a bezpečné migrace na novou platformu a zajištění plné kompatibility řešení s ostatními částmi sítě CS kupující požaduje dodání firewallové platformy Cisco Firepower. Dalším úkonem dodavatele v rámci předmětu plnění bude vlastní provedení migrace firewallové soustavy a integrace nahrazených ASA5545X firewallů do stávajícího VPN řešení složených z ASA5515X, čímž bude rozšířena kapacita VPN řešení. Dále je požadováno dodání a implementace centrálního managementu soustavy perimetru ve formě dvou HW serverů pro zajištění vysoké dostupnosti.

Dodané firewallové řešení musí splňovat následující principy:

- V primárním datovém centru je požadováno nasazení firewallů v režimu HA (High Availability, tedy dva firewally)
- V záložním datovém centru není požadováno nasazení firewallu v režimu HA (zde bude jeden firewall)
- Firewallové řešení musí obsahovat současné bezpečnostní funkce, tedy obsahovat minimálně ochranu formou IPS, Anti-Malware, a URL Filteru
- Firewallové řešení musí podporovat snadnou migraci ACL a NAT pravidel ze současného řešení
- Veškeré dodané firewally, musí být spravovány management systémem, který umožňuje jednotnou centrální správu. Management je požadován formou HW serveru
- Centrální management musí být nasazen v režimu HA (tedy dva HW servery)

Součástí nabídky a nabídkové ceny musí být podpora výrobce a požadované subskripce na 3 roky. Dále pak musí být součástí všechny služby související se zprovozněním celkového řešení a předání kupujícímu do rutinního provozu, zejména pak:

1. Doprava do místa instalace
2. Instalace a konfigurace dodaných firewallů a centrálního managementu
3. Migrace konfigurace ze stávajících ASA5545X na nové firewally

4. Integrace ASA5545X zařízení do stávajícího VPN řešení

Kupující upozorňuje, že implementace řešení bude probíhat za plného provozu jako náhrada stávajícího řešení a bude probíhat právě a jedině zásahem do stávající LAN a bezpečnostní infrastruktury. Je požadována minimalizace plánovaných výpadků a jejich provádění mimo běžnou pracovní dobu. Kupující dále upozorňuje, že předmět plnění souvisí s užitím, správou, či rozvojem Kritické informační infrastruktury ve smyslu ustanovení § 2, písm. b) nebo d) zákona č. 181/2014 Sb. o kybernetické bezpečnosti. Jakékoliv neodborné zásahy mohou mít zásadní dopad na chod organizace kupujícího.

Požadavky kupujícího na poskytnuté řešení

Navrhované řešení musí splňovat zde uvedená kritéria a zároveň splňovat, či převyšovat kritéria uvedená v Příloze č. 2 – Podrobná technická specifikace – tabulka.

Kupující požaduje následující práce:

1. Prodávající zajistí zpracování projektové dokumentace, která bude obsahovat minimálně:
    a. manažerský souhrn,
    b. popis cílového stavu řešení,
    c. harmonogram,
    d. popis implementačních kroků nového řešení,
    e. akceptační testy.
2. Realizaci projektu, která předpokládá následující činnosti:
    a. nasazení centrálních managementů firewallů v obou datových centrech
    b. nasazení dodaných firewallů v obou datových centrech
    c. provedení migrace stávajících bezpečnostních bran ASA5545X na dodavatelem poskytnuté řešení,
    d. provedení migrace přístupových pravidel, routovacích pravidel a NAT ze stávající bezpečnostní brány,
    e. provedení konfigurace filtrování webových dotazů (URL),
    f. implementaci filtrování blacklistovaných IP adres doménových jmen a URL,
    g. nasazení a optimalizaci IPS do prostředí GŘC,
    h. implementaci ochrany proti průchodu malware a škodlivého kódu do vnitřní sítě GŘC,
    i. nastavení vazeb na stávající zdroje (databáze) informací o uživatelích a autentizační servery,
    j. implementace monitoringu všech úspěšných a neúspěšných spojení vytvořených přes bezpečnostní bránu,
    k. integraci na cloud konzoli Cisco AMP For Endpoints
    l. integraci ASA5545X do stávajícího řešení VPN
    m. přenos Site-To-Site VPN
    n. přenos Anyconnect VPN
3. Školení informatiků kupujícího v rozsahu 1 MD.
4. Vytvoření provozní dokumentace.
5. Návrh a provedení akceptačních testů.

Technická specifikace předmětu veřejné zakázky

Veškerý hardware a software dodaný v rámci předmětu plnění musí být určen pro český trh, musí být dodán zcela nový, plně funkční a kompletní včetně příslušenství, vše podle uvedených technických podmínek.

Kupující upozorňuje na skutečnost, že technické parametry jednotlivého hardwaru uvedené v příloze č. 2 jsou uvedeny jako minimální požadavky kupujícího, které musí předměty plnění splňovat a kterými musí zařízení disponovat.

Pokud jsou v technické specifikaci obsaženy požadavky nebo odkazy na jednotlivá obchodní jména, zvláštní označení podniku, zvláštní označení výrobků, výkonů anebo obchodních materiálů, která platí pro určitý podnik nebo organizační jednotku za příznačné, popř. patenty a užité vzory, jsou uvedeny pouze pro upřesnění a přiblížení technických parametrů a kupující umožňuje použití i kvalitativně a technicky obdobného řešení s plně srovnatelnými nebo i převyšujícími parametry.

Podrobný popis požadovaných technických parametrů a specifikací se nachází v Příloze č. 2 této smlouvy (Podrobná technická specifikace-tabulka).

Specifikace dodávky

- 3 kusy firewallů včetně příslušného software dle technické specifikace,
- 2 kusy serverů včetně příslušného software pro centrální management systému dle technické specifikace
- tříletý servis na dodaná zařízení s reakcí 8x5 NBD, v pracovní době následující den,
- tříleté subscripce na URL filtering pro všechny dodané firewally
- tříleté subscripce na funkcionalitu prevence hrozeb včetně IPS a Anti-Malware dle technické specifikace pro všechny dodané firewally
- vypracování projektu řešení včetně vytvoření projektové a provozní dokumentace
- realizace projektu – instalace a konfigurace navrženého firewallového řešení s využitím dodávaného i stávajícího hw a sw včetně provedení migrace stávajících pravidel a nastavení a návrh a provedení akceptačních testů
- školení správců systému v rozsahu jednoho člověkodne

Modernizace a rozšíření kapacity firewallových soustav na perimetru sítě CS

Požadovaná funkcionalita / vlastnost		Nabízené řešení splňuje / nesplňuje požadavek kupujícího (doplní uchazeč ANO / NE)	Hodnota nabízeného technického parametru nebo způsob zabezpečení technického požadavku
Firewall - tři kusy zařízení včetně tříleté podpory výrobce			
Cisco Firepower 2130 (https://www.cisco.com/c/en/us/products/security/firewalls/index.html#Resources)			
Výkonové paramentry a funkce FW na perimetru			
Formát zařízení	Appliance, 1RU	ANO	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	12	ANO	12x 1Gb 10/100/1000 BaseT Ethernet rozhraní, standardně osazených
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	4	ANO	4x 10Gb SFP+ rozhraní, standardně osazených
Minimální počet 10Gb SFP+ rozhraní portů pro data, možnost rozšíření	8	ANO	Možnost rozšíření o 8x 10Gb SFP+ rozhraní pomocí modulu
Podporovaný počet současně otevřených spojení aplikační FW	2M	ANO	2M spojení přes aplikační FW (AVC)
Rychlost vytváření nových spojení přes aplikační FW	24K/s	ANO	27K conn/s přes aplikační FW (AVC)
Propustnost aplikačního FW (next-gen FW)	4,75 Gbps	ANO	5 Gbps (profil TCP 1024B)
Propustnost aplikačního FW + IPS (next-gen FW, IPS)	4,75 Gbps	ANO	5 Gbps (profil TCP 1024B)
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	1,7 Gbps	ANO	1,7 Gbps (profil TCP 450B)
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	1,7 Gbps	ANO	1,7 Gbps (profil TCP 450B)
Minimální počet VPN peerů	7500	ANO	FW podporuje 7500 VPN peerů
Propustnost IPSec VPN	1,5 Gbps	ANO	1,6 Gbps (profil TCP 1024B)
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano	ANO	Zařízení splňuje parametr
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO	Zařízení splňuje parametr
Podpora 802.1Q tagovaných rámců	Ano	ANO	Zařízení splňuje parametr
Podporovaný počet VLAN	Min. 1024	ANO	FW podporuje 1024 VLAN
Podpora stateful failover	active/standby	ANO	Zařízení podporuje active/standby i clusterování pro zajištění redundance
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO	ANO, funkce se nazývá EtherChannel

Dynamické směrování - podpora minimálně RIP, OSPF, BGP	Ano	ANO	Zařízení splňuje parametr
Podpora IPv6 dynamického směrování – minimálně OSPFv3, BGP	Ano	ANO	Zařízení splňuje parametr
Podpora Policy based Routing	Ano	ANO	Zařízení splňuje parametr
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO	ANO, protokol PxGrid, nebo REST API.
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	ANO	Zařízení splňuje parametr
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano	ANO	Zařízení splňuje parametr
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	ANO	Zařízení splňuje parametr

Funkce Next-Gen FW			
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO	Zařízení splňuje parametr
Podpora pasivního monitorování (TAP režim)	Ano	ANO	Zařízení splňuje parametr
Podporovaných aplikací	Min. 3000	ANO	FW podporuje 4000+ aplikací
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO	Zařízení splňuje parametr
URL kategorie	80	ANO	FW podporuje 80+ URL kategorií
Kategorizovaných světových URL	280M	ANO	FW podporuje 280M+ světových URL
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano	ANO	Zařízení splňuje parametr
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO	Zařízení splňuje parametr
Filtrace podle reputace serverů	Ano	ANO	FW podporuje 5 reputačních úrovní webových stránek
SSL inspekce (dekrypce/enkrypce)	Ano	ANO	ANO, SSL dekrypce/enkrypce je realizována na HW úrovni
Security Inteligence database – známé uzly botnet sítí C&C	Ano	ANO	ANO, FW pravidelně aktualizuje Security Intelligence DB, aby blokoval komunikace na nebezpečné servery v internetu
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	ANO	ANO, FW pravidelně aktualizuje Security Intelligence DB, aby blokoval komunikace na nebezpečné servery v internetu
Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	Ano	ANO	ANO, FW pravidelně aktualizuje Security Intelligence DB, aby blokoval komunikace na nebezpečné servery v internetu
Možnost integrovat vlastní reputační databáze	Ano	ANO	Zařízení splňuje parametr
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO	Zařízení splňuje parametr

Podpora filtrování provozu			
Podpora filtrace IPv4, IPv6	Ano	ANO	Zařízení splňuje parametr
Podpora filtrace podle bezpečnostních zón	Ano	ANO	Zařízení splňuje parametr
Podpora filtrace podle VLAN tagů	Ano	ANO	Zařízení splňuje parametr
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO	Zařízení splňuje parametr

Podpora filtrace podle aplikace, kategorie rizikovosti a business relevance	Ano	ANO	Zařízení splňuje parametr
Podpora filtrace podle bezpečnostních skupin naučených z RADIUS serveru	Ano	ANO	Zařízení splňuje parametr
Podpora konfigurace logování per přístupové pravidlo	Ano	ANO	Zařízení splňuje parametr
Podpora aplikace IPS politik per přístupové pravidlo	Ano	ANO	Zařízení splňuje parametr

Funkce Intrusion Prevention Systém a Anti-Malware protection			
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO	FW umožňuje granulárně určovat provoz pro inspekci IPS modulem per přístupové pravidlo
Podpora IDS režimu – pasivního monitorování (TAP režim)	Ano	ANO	IPS lze nasadit v pasivním, IDS i TAP režimu
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	ANO	Zařízení splňuje parametr
Podpora různých IPS politik pro různé typy provozu	Ano	ANO	FW umožňuje granulárně určovat provoz pro inspekci IPS modulem per přístupové pravidlo
Inspekce pro IPv4 i IPv6	Ano	ANO	FW podporuje inspekci IPv4 i IPv6
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano	ANO	IPS signatury jsou pravidelně aktualizovány a doplňovány výrobcem, aby reflektovaly aktuální hrozby; IPS obsahuje signatury pro všechny zmíněné skupiny útoků
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	ANO	FW automaticky aktualizuje všechny zmíněné informace, aby reflektoval aktuální hrozby
Podpora importu komunitních filtrů/signatur Snort	Ano	ANO	Zařízení splňuje parametr
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO	Zařízení splňuje parametr
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	ANO	Zařízení splňuje parametr
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano	ANO	ANO, pomocí DNS politiky
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano	ANO	IPS obsahuje signatury, které chrání proti zmíněným útokům
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	ANO	Signatury obsahují informace jako: popis, dokumentace, odkaz na CVE apod.
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano	ANO	ANO, Snort umožňuje konfiguraci preprocesorů pro základní funkce DLP
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	ANO	FW podporuje nastavení více vrstev IPS politik
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	ANO	FW umožňuje automaticky generovat doporučené sady IPS signatur na základě učení sítě

Možnost definice uživatelské vrstvy politik	Ano	ANO	FW umožňuje konfigurace uživatelské vrsvy IPS politik
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	ANO	Zařízení splňuje parametr
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware, nezávislé na aktuálních databázích AV dodavatelů třetích stran	Ano	ANO	Inline ochranu lze implementovat pomocí vlastních funkcí ochrany proti malwaru
Kontrola souborů pomocí hash funkce (SHA256) vůči cloudu výrobce za účelem zjištění dispozice souboru	Ano	ANO	FW podporuje ochranu proti malwaru vůči cloudu výrobce pomocí SHA256 hashe
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano	ANO	FW podporuje ochranu proti zero-day malwaru
Retrospektivní ochrana prostředí – pokud se dispozice souboru změní na Malware až po průchodu souboru, IPS vygeneruje alarm	Ano	ANO	FW vygeneruje alarm, pokud je soubor určen jako malware i pokud soubor již prošel FW
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	ANO	ANO, transparentní mód je podporován
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	ANO	FW umožňuje generovat alarm, pokud detekované zařízení není compliant
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	ANO	Remediation moduly jsou podporovány
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	ANO	FW umožňuje nasazení vlastních remediation modulů
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	ANO	ANO, FW pravidelně aktualizuje Security Intelligence DB, aby blokoval komunikace na nebezpečné servery v internetu

Možnosti integrace a další funkcionality Firewallu			
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	ANO	ANO, rozhraní pro příjem netflow záznamů je podporováno
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano	ANO	Zařízení splňuje parametr
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO	ANO, pomocí funkce TCP reassembly
Podpora NAT64 a DNS64	Ano	ANO	Zařízení splňuje parametr
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO	ANO, pomocí funkce Network Discovery
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení a musí poskytovat minimálně tyto informace: Typ zařízení, Operační systém, Dodavatel OS, Použité síťové protokoly, Použité síťové služby, Otevřené porty síťových služeb a Potenciální zranitelnosti	Ano	ANO	ANO, pomocí funkce Network Discovery

Přehled o síťových spojeních musí poskytovat minimálně tyto informace: Čas startu a konce flow, Akce (allow, deny,..), Důvod případného blokování, Zdrojovou a cílovou adresu, Vstupní a výstupní zónu, Vstupní a výstupní rozhraní, Zdrojový a cílový port, Aplikační protokol, IPS událost (pokud vznikne), Rizikovou úroveň IPS události, Použitou síťovou aplikaci, Rizikovost aplikace, "Business impact" aplikace a Množství přenesených dat	Ano	ANO	ANO, zmíněné údaje jsou zahrnuty ve výpisu detekovaných spojení.

Funkcionalita VPN			
Podpora IPSec VPN	Ano	ANO	Zařízení splňuje parametr
IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol	Ano	ANO	Zařízení splňuje parametr
Podpora nového protokolu pro výměny klíčů IKEv2	Ano	ANO	Zařízení splňuje parametr
Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256	Ano	ANO	Zařízení splňuje parametr
Podpora kontrolních mechanizmů: MD5, SHA	Ano	ANO	Zařízení splňuje parametr
Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256	Ano	ANO	Zařízení splňuje parametr
Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384	Ano	ANO	Zařízení splňuje parametr
Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA	Ano	ANO	Zařízení splňuje parametr

Centrální management Firewallu - dva kusy zařízení včetně tříleté podpory výrobce			
Firepower Management Center 2600 (https://www.cisco.com/c/en/us/products/security/firepower-management-center/index.html#Resources)			
Funkcionality Centrálního managementu			
HW appliance	Ano	ANO	ANO, 1 RU server
Podpora High-Availability	Ano	ANO	ANO, podpora HA v režimu Active/Standby
Minimální počet spravovaných sensorů/FW	300	ANO	FMC umožňuje spravovat až 300 senzorů/FW
Minimální kapacita IPS eventů	60M	ANO	FMC má kapacitu až 60 mil. IPS eventů
Minimální počet Flows per Second	12K/s	ANO	FMC umožňuje přijímat až 12 tis. eventů/s
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	ANO	FMC je spravováno přes webové rozhraní
Přístup ke GUI http/https protokolem	Ano	ANO	Zařízení splňuje parametr
Možnost centrální správy při nasazení více firewallů	Ano	ANO	Všechny spravované senzory/FW jsou spravovány centrálně přes FMC
Možnost sdílených bezpečnostních politik	Ano	ANO	Bezpečností politiky lze sdílet přes více FW

Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	ANO	Všechny spravované senzory/FW jsou spravovány centrálně přes FMC
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	ANO	FMC umožňuje zobrazovat logy a události všech spravovaných senzorů/FW
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	ANO	Zařízení disponuje celou řadou nástrojů pro troubleshooting jako testování průchodu paketů nebo packet capture
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap	Ano	ANO	Zařízení splňuje parametr
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	ANO	Zařízení disponuje celou řadou nástrojů pro troubleshooting jako testování průchodu paketů nebo packet capture
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod.	Ano	ANO	FMC ukládá všechny události do interní DB, kterou lze využít na dlouhodobější uchovávání dat, generování reportů a korelaci.
Centrální management musí být schopný dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	ANO	Všechny spravované senzory/FW jsou kompletně spravovány centrálně přes FMC; konfigurované politiky lze sdílet přes více senzorů/FW
Centrální management musí být schopný poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	ANO	FMC centrálně distribuuje všechny bezpečnostní aktualizace jako IPS signatury, AV signatury, URL, nebo Security Intelligence DB; aktualizace lze vyvolat manuálně, nebo podle časového harmonogramu
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI Centrálního managementu	Ano	ANO	FMC disponuje bohatým dashboardem a reportingem, který umožňuje zobrazovat nasbíraná data v tabulkách či grafech
Přehledy a statistiky v Centrálním managementu lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	ANO	ANO, filtrování v eventech je podporováno včetně možnosti ukládání filtrů a jejich pozdějšího vyvolání
Centrální management musí být schopný vytvářet reporty manuálně a podle časového harmonogramu	Ano	ANO	Reporty lze vytvářet manuálně nebo dle časového harmonogramu
Pro reporty lze definovat template definující formát a obsah reportu	Ano	ANO	Zařízení splňuje parametr
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	ANO	Zařízení splňuje parametr
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	ANO	Zařízení splňuje parametr
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	ANO	ANO, dashboardy a reporty jsou navzájem prolinkované
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	ANO	Zařízení splňuje parametr
Centrální management musí být schopný integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	ANO	ANO, FMC lze integrovat s externími DB jako např.: Microsoft Active Directory, pro vytváření bezpečnostních politik na základě identity a skupiny uživatele.
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	ANO	Zařízení splňuje parametr

Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	ANO	Zařízení splňuje parametr
Podpora Event Streamer API (eStreamer) pro sdílení informací s externími systémy - minimálně pro tyto SIEM: ArcSight, Novell Sentinel, Q1Labs-QRadar, Log Rhythm SIEM 2.0, LogLogic a Splunk	Ano	ANO	Zařízení splňuje parametr
Podpora integrace s autentizačním RADIUS serverem pomocí zabezpečeného protokolu SSL/TLS	Ano	ANO	ANO, pomocí protokolu PxGrid
Možnost karantény konzového uživatele pomocí RADIUS serveru při stažení malware	Ano	ANO	ANO, možnost blokování přímo na FW nebo pomocí protokolu PxGrid přes RADIUS server
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	ANO	Zařízení splňuje parametr
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	ANO	Zařízení splňuje parametr
Podpora řízeného přístupu podle rolí administrátorů	Ano	ANO	ANO, zařízení podporuje RBAC
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	ANO	Zařízení splňuje parametr
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a Centrálním managementu (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	ANO	ANO, FMC umožňuje sledovat svůj stav a stav spravovaných senzorů/FW a tvorbu politik na sledování různých HW a SW chyb a limitů; na poruchy lze reagovat různými způsoby, např. generováním alarmu
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	ANO	ANO, FMC umožňuje sledovat svůj stav a stav spravovaných senzorů/FW a tvorbu politik na sledování různých HW a SW chyb a limitů; na poruchy lze reagovat různými způsoby, např. generováním alarmu
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory/firewally nebo Centrální management	Ano	ANO	ANO, FMC umožňuje konfiguraci různých politik sledujících stav spravovaného zařízení; každé spravované zařízení může mít vlastní politiku
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano	ANO	FMC umožňuje zobrazit trajektorii malwaru, jeho šíření po síti, zdroj nákazy apod.