Hasičský záchranný sbor Moravskoslezského kraje				
EVIDENCE SMLUV				
HMSK	SML	55	2021	
		poř. číslo	rok	doba plnění
Evidence v SSD				

KUPNÍ SMLOUVA

I. Smluvní strany

Česká republika - Hasičský záchranný sbor Moravskoslezského kraje
Sídlo: Výškovická 40, 700 30 Ostrava-Zábřeh
IČO: 70884561
DIČ: CZ 70884561 (není plátcem DPH)
Zastoupený: brig. gen. Ing. Vladimírem Vlčkem, Ph.D., MBA, ředitelem HZS Moravskoslezského kraje
Bankovní spojení: ČNB Ostrava, č. účtu: 1933881/0710
(dále jen „kupující")

a

VÍTKOVICE IT SOLUTIONS a.s.
Sídlo: Cihelní 1575/14, Ostrava-Moravská Ostrava, 702 00
IČO: 28606582
DIČ: CZ28606582
Zastoupená: [redacted]
Bankovní spojení: Česká spořitelna, a.s., č. účtu: 4312807389/0800
zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě, odd. B, vložka 4229
(dále jen „prodávající")

II. Základní ustanovení

1. Smluvní strany uzavírají tuto smlouvu v souladu s ustanoveními § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „OZ") a dohodly se, že tento závazkový vztah, rozsah a obsah vzájemných práv a povinností z této smlouvy vyplývajících se bude řídit příslušnými ustanoveními citovaného zákoníku, nestanoví-li tato smlouva jinak.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I. této smlouvy a taktéž oprávnění k podnikání jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení druhé smluvní straně.
3. Smluvní strany prohlašují, že si před uzavřením smlouvy vzájemně sdělily veškeré jim známé skutkové a právní okolnosti, které by mohly být významné ve vztahu k uzavření této smlouvy nebo k plnění z této smlouvy vyplývajícímu.
4. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.

III. Předmět smlouvy

1. Předmětem této smlouvy je výměna centrální bezpečnostní infrastruktury - firewallů včetně nasazení pokročilých bezpečnostních funkcionalit (NGFW) s centrálním managementem, komplexní návrh řešení včetně zpracování scénáře implementace, migrace síťového provozu do nové infrastruktury , jak je blíže specifikováno v příloze č. 1 této smlouvy (dále jen „zboží").

2. Prodávající se zavazuje kupujícímu zboží dodat a umožnit mu nabýt vlastnické právo ke zboží. Součástí dodání je i předání dokladů, které se ke zboží vztahují, a doprava zboží do místa plnění.
3. Vlastnické právo ke zboží přechází na kupujícího okamžikem odevzdání a převzetí zboží kupujícím v místě plnění.
4. Smluvní strany prohlašují, že předmět smlouvy není plněním nemožným a že smlouvu uzavřely po pečlivém zvážení všech možných důsledků.
5. Podkladem pro uzavření této smlouvy je nabídka prodávajícího ze dne 6.11.2020, která byla na základě zadávacího řízení č. 164/2020/OŘ vybrána jako nejvýhodnější.

IV. Kupní cena

1. Kupující se zavazuje zboží převzít a zaplatit prodávajícímu kupní cenu.
2. Kupní cena je stanovena dohodou smluvních stran a činí:

cena bez DPH	3 937 723,00 Kč
DPH 21 %	826 921,83 Kč
cena včetně DPH	4 764 644,83 Kč

3. Podrobná kalkulace celkové kupní ceny tvoří přílohu č. 2 této smlouvy.
4. Sjednaná kupní cena je konečná a zahrnuje veškeré náklady spojené s koupí zboží, a to zejména dopravu zboží do místa plnění podle čl. VI. této smlouvy, instalaci, instruktáž obsluhy, clo, skladování, balné atd..
5. Cena je stanovena jako nejvýše přípustná při sazbě DPH ve výši 21%, přičemž sazba DPH bude v případě její změny stanovena v souladu s platnými právními předpisy.

V. Čas plnění

Prodávající je povinen dodat kupujícímu zboží do 120 kalendářních dnů od nabytí účinnosti uzavřené smlouvy.

VI. Místo plnění

Místem plnění podle této smlouvy je Integrované bezpečnostní centrum Moravskoslezského kraje, ul. Nemocniční 3328/11, 702 00 Ostrava – Moravská Ostrava.

VII. Způsob dodání zboží

1. Zboží je dodáno v okamžiku převzetí zboží pověřeným zástupcem kupujícího v místě plnění uvedeném v této smlouvě. Pověřený zástupce kupujícího potvrdí převzetí zboží na dodacím listu, předávacím protokolu nebo jiném obdobném dokladu.
2. Kupující se zavazuje zboží, dodané řádně a včas, převzít a zaplatit za něj kupní cenu.
3. Kupující při převzetí zboží provede kontrolu:
   a) dodané značky, typu, druhu,
   b) dodaného množství,
   c) zjevných jakostních vlastností,
   d) zda nedošlo k poškození zboží při přepravě,
   e) dodaných dokladů.
4. V případě zjištěných zjevných vad zboží může kupující odmítnout jeho převzetí, což řádně i s důvody potvrdí na příslušném dokladu. Na následné předání zboží se použijí ustanovení tohoto článku obdobně.

VIII. Jakost, záruka za jakost, vady zboží

1. Prodávající je povinen dodat zboží v množství, druhu, jakosti, provedení stanovenými touto smlouvou a podle technických parametrů a obchodních podmínek sjednaných v této smlouvě. Smluvní strany se dohodly na I. jakosti dodaného zboží. Prodávající je povinen dodat zboží nové, nepoužité, v okamžiku dodání nesmí být zboží starší 12 měsíců.
2. Prodávající není oprávněn dodat větší než sjednané množství zboží, ustanovení § 2093 OZ se nepoužije.
3. Prodávající prohlašuje, že zboží nemá právní vady podle § 1920 OZ.
4. Poruší-li prodávající povinnosti stanovené v odst. 1 tohoto článku, jedná se o vady plnění.
5. V případě dodání vadného plnění se práva a povinnosti smluvních stran řídí ustanoveními § 2099 a násl. OZ.
6. Smluvní strany se dohodly na záruční době 60 měsíců.
7. Komunikaci v rámci záruky je prodávající povinen poskytovat v českém jazyce.
8. Záruční doba začíná běžet dnem předání zboží kupujícímu bez vad a nedodělků.
9. Záruční doba neběží po dobu, po kterou nemůže kupující zboží řádně užívat pro vady, které jsou způsobilé založit práva kupujícího z vadného plnění.
10. Veškeré vady zboží je kupující povinen oznámit prodávajícímu bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení o vadě zaslaného na adresu prodávajícího: telefonicky na tel. č. [redacted] (v režimu 24x7), e-mailem na [redacted]
11. Prodávající je povinen kupujícímu písemně potvrdit, kdy bylo právo z vadného plnění uplatněno, způsob provedení opravy a dobu trvání opravy.
12. V záruční době prodávající započne s odstraněním vady neprodleně do 1 hodiny od oznámení o vadě, pokud se smluvní strany nedohodnou jinak. Prodávající je povinen zajistit nejpozději do 12 hodin od oznámení vady plnou funkčnost systému překlenutím vady, a to až do úplného odstranění vady, pokud se smluvní strany nedohodnou jinak.
13. V rámci záruky musí být vada odstraněna do 4 pracovních dnů od oznámení vady, pokud se smluvní strany nedohodnou jinak.
14. V případě, kdy vadu nebude možné odstranit ve lhůtě dle odst. 13, je prodávající povinen poskytnout kupujícímu pro překlenutí závady zdarma náhradní zařízení (zboží) se stejnými či vyššími parametry, a to až do doby ukončení opravy a předání opraveného zboží kupujícímu.
15. Nebezpečí škody na zboží přechází na kupujícího okamžikem převzetí zboží.
16. Prodávající je povinen nahradit kupujícímu škodu, která vznikne porušením smluvní povinnosti prodávajícího nebo vadným plněním, a to v plné výši. Prodávající je rovněž povinen kupujícímu nahradit náklady, které kupujícímu vzniknou při uplatňování práv na náhradu škody.

IX. Platební podmínky

1. Smluvní strany nesjednávají zálohy na kupní cenu.
2. Podkladem pro úhradu kupní ceny dodaného zboží bude faktura, která bude mít náležitosti daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále také „faktura"). Kupující tímto souhlasí s použitím daňového dokladu v elektronické podobě.
3. Faktura musí kromě zákonem stanovených náležitostí obsahovat také:
   a) označení smlouvy a datum jejího uzavření
   b) označení banky a čísla účtu, na který musí být zaplaceno
   c) kontaktní údaje prodávajícího pro záležitosti fakturace

d) součástí faktury musí být dodací list, předávací protokol nebo jiný obdobný doklad včetně soupisu jednotlivých položek, podepsaný zástupci obou smluvních stran, potvrzující, že zboží podle této smlouvy bylo řádně dodáno.

4. Faktura bude prodávajícím vystavena po odevzdání a převzetí zboží podle této smlouvy. Lhůta splatnosti faktury je dohodou stanovena na 30 kalendářních dnů ode dne doručení faktury kupujícímu. Stejná lhůta splatnosti platí i při placení jiných plateb (např. úroků z prodlení, smluvních pokut, náhrad škody aj.).
5. Faktura v listinné podobě musí být doručena na adresu kupujícího na ul. Výškovická 40, 700 30 Ostrava-Zábřeh, a faktura v elektronické podobě musí být doručena na e-mailovou adresu: uctarna@hzsmsk.cz.
6. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude chybně vyúčtována cena nebo DPH, je kupující oprávněn bez zaplacení faktury před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy. Ve vrácené faktuře vyznačí důvod vrácení. Prodávající provede opravu vystavením nové faktury. Od doby odeslání vadné faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží opět ode dne doručení nově vyhotovené faktury kupujícímu.
7. Smluvní strany se dohodly, že platba bude provedena bezhotovostním převodem z účtu kupujícího na číslo účtu uvedené prodávajícím na faktuře bez ohledu na číslo účtu uvedené v čl. I. této smlouvy.
8. Povinnost zaplatit cenu zboží je splněna dnem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.
9. Pokud kupující uplatní nárok na odstranění vady zboží ve lhůtě splatnosti faktury, není kupující povinen až do odstranění vady zboží uhradit cenu zboží. Okamžikem odstranění vady zboží začne běžet nová lhůta splatnosti faktury.

X. Podstatné porušení smlouvy

1. Smluvní strany pokládají za podstatné porušení této smlouvy:
   a) prodlení prodávajícího se splněním ve sjednaném čase plnění podle čl. V. této smlouvy,
   b) nedodání zboží v požadované kvalitě nebo množství podle této smlouvy,
   c) nevyřešení zjištěných vad v souladu s čl. VIII. této smlouvy ve sjednané lhůtě.
2. V případě podstatného porušení smlouvy ze strany prodávajícího je kupující oprávněn od této smlouvy odstoupit podle čl. XII.

XI. Sankční ujednání

1. V případě prodlení prodávajícího s dodáním zboží je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,2 % z celkové kupní ceny vč. DPH za každý i započatý den prodlení.
2. V případě prodlení kupujícího se zaplacením dohodnuté kupní ceny je kupující povinen zaplatit prodávajícímu úrok z prodlení ve výši 0,05 % z dlužné částky za každý i započatý den prodlení.
3. V případě nedodržení dohodnuté lhůty k odstranění vad dle čl. VIII. odst. 13 této smlouvy, jestliže se tyto vady projevily v záruční době, je prodávající povinen kupujícímu uhradit smluvní pokutu ve výši 1000,- Kč za každý i započatý den prodlení s odstraněním každé vady.
4. Zánik závazku pozdním plněním neznamená zánik nároku na smluvní pokutu za prodlení s plněním.
5. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně.
6. Smluvní pokuty je kupující oprávněn započíst proti pohledávce prodávajícího.

7. Smluvní pokuty sjednané touto smlouvou zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé smluvní straně škoda, kterou lze vymáhat samostatně.

XII. Odstoupení od smlouvy

1. Odstoupení od smlouvy se řídí ustanovením § 2001 a násl. OZ, pokud není dále stanoveno jinak.
2. Kupující je oprávněn odstoupit od smlouvy, jestliže se prodávající rozhodnutím soudu ocitne v úpadku dle zákona č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů.
3. Účinky každého odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně. Odstoupení od smlouvy se nedotýká zejména nároku na náhradu škody, smluvní pokuty a povinnosti mlčenlivosti.
4. Prodávající podpisem této smlouvy prohlašuje, že není veden v registru nespolehlivých plátců DPH vedeném Ministerstvem financí České republiky. V případě, že je toto prohlášení nepravdivé nebo v případě, že bude prodávající dodatečně zapsán v registru nespolehlivých plátců DPH v průběhu plnění této smlouvy a nevyrozumí o tom ihned kupujícího, má kupující právo od smlouvy odstoupit v souladu s odst. 3 tohoto článku.

XIII. Závěrečná ujednání

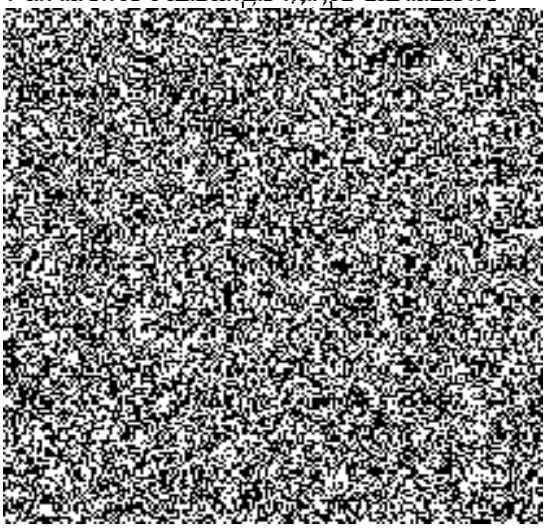
1. Tato smlouva se řídí právním řádem České republiky. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací smlouvy budou řešeny nejprve smírnou cestou – dohodou. Nedojde-li k dohodě, budou spory řešeny v soudním řízení před příslušnými obecnými soudy České republiky.
2. Prodávající není oprávněn bez předchozího písemného souhlasu kupujícího postoupit tuto smlouvu, její část nebo práva a povinnosti z této smlouvy třetí osobě.
3. Prodávající bez jakýchkoliv výhrad souhlasí se zveřejněním své identifikace a dalších údajů uvedených ve smlouvě včetně ceny zboží.
4. Změnit nebo doplnit tuto smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této kupní smlouvy a podepsány oprávněnými zástupci obou smluvních stran.
5. Pro případ, že ustanovení této smlouvy oddělitelné od ostatního obsahu se stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečných odkladů nahradit takové ustanovení novým. Případná neplatnost některého z takovýchto ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení.
6. Prodávající se zavazuje, že jakékoliv informace, které se dověděl v souvislosti s plněním předmětu smlouvy, neposkytne bez předchozího písemného souhlasu třetím osobám ani je nepoužije v rozporu s účelem této smlouvy, ledaže se jedná o informace, které jsou veřejně přístupné nebo o případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu. Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na dodání zboží dle této smlouvy, odpovídá prodávající, jako by povinnost porušil sám. Povinnost mlčenlivosti trvá i po splnění této smlouvy.
7. Smluvní strany shodně prohlašují, že si tuto smlouvu před jejím podepsáním přečetly, že byla uzavřena po vzájemném projednání, nebyla uzavřena v tísni ani za jednostranně nevýhodných podmínek a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.
8. Tato smlouva podléhá povinnosti uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a

o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, přičemž smluvní strany souhlasí s jejím uveřejněním v plném rozsahu. Uveřejnění této smlouvy v registru smluv zajistí kupující.

9. Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv.
10. Smluvní strany uzavírají tuto smlouvu v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Osobní údaje uvedené v této smlouvě budou použity pouze pro účely plnění této smlouvy a při uveřejnění smlouvy budou anonymizovány.
11. Vše, co bylo dohodnuto před uzavřením smlouvy, je právně irelevantní a mezi stranami platí jen to, co je dohodnuto v této smlouvě.
12. Tato smlouva je vyhotovena v elektronické podobě. Smluvní strana podepisující tuto smlouvu jako druhá v pořadí je povinna prokazatelně doručit podepsanou smlouvu druhé smluvní straně.
13. Nedílnou součástí této smlouvy je příloha č. 1 – technická specifikace a příloha č. 2 – cenová kalkulace.

Podpisy smluvních stran:

za kupujícího:
brig. gen. Ing. Vladimír Vlček, Ph.D., MBA
ředitel
HZS Moravskoslezského kraje



příloha č. 1 – technická specifikace

Technická specifikace obnovy bezpečnostní infrastruktury sítě IBC Moravskoslezského kraje

Stávající síťové prvky a infrastruktura týkající se bezpečnosti a řízení provozu sítě integrovaného bezpečnostního centra Moravskoslezského kraje (dále IBC MSK) je v permanentním rutinním provozu od roku 2010. V rámci této veřejné zakázky se jedná zejména o centrální FWSM moduly v Cisco C6500 a perimetrové firewally Cisco ASA 5510, u kterých již není možno zajistit odpovídající technickou podporu, resp. podpora je již ukončena. Tyto prvky jsou klíčovou součástí síťové infrastruktury IBC a slouží k segmentaci a řízení vnitřního provozu sítě a oddělení vnitřní sítě IBC MSK od veřejných komunikačních sítí a spolupodílí se také na řízení přístupů z vnějších sítí. Vzhledem k charakteru provozu pracují tyto prvky ve failover modu.

Přemětem řešení je dodání:

- 2 ks Next-Generation Firewallu provozovaného ve vysoké dostupnosti včetně aktivované funkcionality IPS (Intrusion Prevention System), reputační databáze (Security Inteligence) a AMP (Advanced Malware Protection) – FWIPS
- 2 ks Next-Generation Firewallu provozovaného ve vysoké dostupnosti, požadována je funkcionalita AVC (application visibility and control) - FWVSS
- Centrální hardwarový management pro správu firewallů ve vysoké dostupnosti (minimálně pro 6 zařízení)
- Webová proxy ve vysoké dostupnosti včetně anti-malware ochrany (minimálně pro 100 uživatelů) s jednotným centrálním managementem pro instalaci do virtuálního prostředí
- Ochrana před nežádoucí komunikací na úrovni DNS a IP adres pro koncové stanice tzv. teleworkers včetně jednotné management konzole
- Řešení anti-malware ochrany pro koncové stanice tzv. teleworkers včetně jednotné management konzole (do 50 uživatelů)
- Centrální incident response konzole, skrze kterou se budou vyčítat/vizualizovat bezpečnostní incidenty a provádět reakce z dodávané dvojice NGFW, webové proxy, a koncových zařízení (teleworkers)
- Doplňující prvky pro integraci nového zařízení do stávající infrastruktury - 2 ks přepínačů pro připojení externích konektivit a 12 ks SFP+ SR, 2 ks WS-X6708-10G-3C do C6500 a 8 ks X2-10GB-SR modul

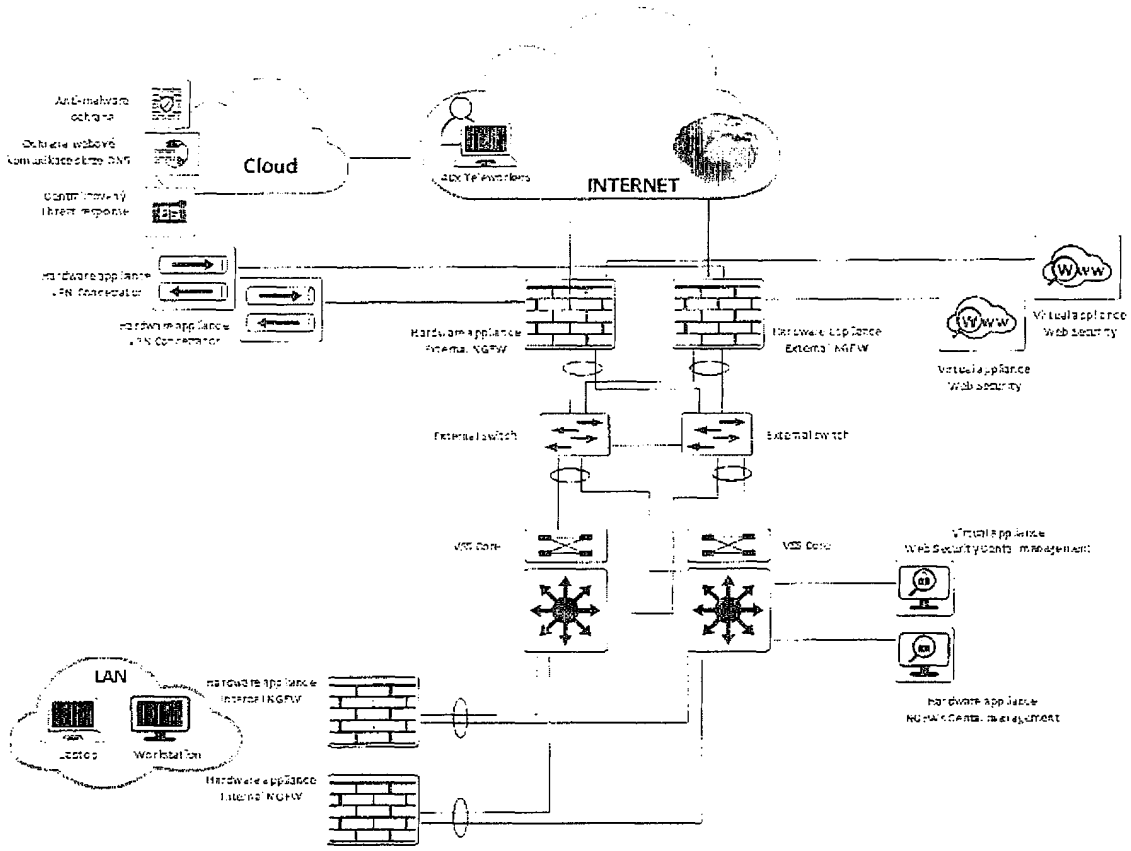
Nedílnou součástí řešení je:

- Analýza stávající konfigurace pravidel na Cisco FWSM, Cisco ASA 5510 s IPS modulem (optimalizace/redukce pravidel)
- Instalace posledního stabilního operačního systému pro dodané NGFW
- Sestavení HA clusteru active/passive pro dvě dvojice NGFW
- Přenesení/rozdělení konfigurace z Cisco FWSM na nové dvě dvojice NGFW
- Instalace centrálního managementu pro správu NGFW v možném multi-tenant režimu pro dodávané dvě dvojice NGFW
- Aktivace a ladění IPS a anti-malware funkcionality na jedné dvojici firewallů
- Instalace webové (content) proxy/centrálního managementu pro zajištění bezpečnosti nad webovým obsahem provozu koncových uživatelů a centrálního managementu včetně aktivace a ladění požadavků na SSL dekrypci
- Typová Instalace anti-malware DNS/IP ochrany pro koncová zařízení teleworkers
- Instalace stacku dvou přepínačů pro propoj s externími společnostmi
- Dodání funkcionalit síťových i koncových zařízení, které se aktivují s časově omezenou licencí tak, aby byla zajištěna plná funkcionalita po dobu 5 let
- Vypracování technické dokumentace odpovídající fázi realizace, požaduje se strukturovaná dokumentace typu Analýza prostředí, Migrační proces, High level a Low level dokument, Akceptační testy, Závěrečná technická dokumentace, tyto dokumenty pro konkrétně nasazovanou technologii v daném prostředí IBC MSK
- integrace do dohledu IBC – CA Spectrum OneClick

Další podmínky realizace

Požaduje se dodání komplexního systému, který bude postaven na HW a SW komponentách jednoho výrobce. Veškeré instalační a konfigurační práce budou probíhat za plného provozu a musí být prováděny tak, aby implementace nových zařízení neměla zásadní vliv na stávající provoz sítě. Součástí ceny dodávky je požadovaná záruka na HW a SW min. 60 měsíců s SLA 24x7 (s výjimkou doplňujících komponent stavajících síťových prvků Cisco C6500) s dobou odezvy 1hod/překlenutí 12hod/ 4 pracovní dny vyřešení, v rámci záruční doby musí být garantována výměna za produkt ve stejné konfiguraci včetně zprovoznění u zadavatele. Pro nahlášení poruch dodavatel poskytne kontaktní místo s možností sledování servisních reportů. Komunikaci v rámci záruky bude dodavatel poskytovat v českém jazyce.

Obecné schéma řešení:



Požadované vlastnosti řešení:

Z důvodu současných požadavků na provoz komunikačních sítí, na zajištění potřebných funkcionalit a zvláště na zajištění bezpečnosti s ohledem na hrozby v této oblasti se požaduje řešení odpovídající standardu dnešní doby. Vedle tradičního filtrování provozu na základě IP adres a komunikačních portů se požaduje využití pokročilých metod zajištění provozu, jeho řízení a zabezpečení prostřednictvím funkcionalit Next-Generation Firewallů (dále NGFW). Jedná se zejména u prvků FWIPS (viz výše) o analýzu a detekci škodlivého provozu na úrovni protokolu HTTP/HTTPS a komunikující aplikace včetně eliminace hrozeb, inspekci síťového provozu s detekcí a ochranou na úrovni síťového provozu (IPS), v oblasti ochrany proti mallware o schopnost aktivace dynamické analýzy (sandboxing) včetně ukládání nebezpečných souborů do karantény a interní korelaci událostí pro zajištění automatické detekce kompromitovaných stanic včetně kontinuální analýzy síťového prostředí s automatickou reakcí na porušení pravidel. Funkce URL filtrace zvláště s ohledem na zátěž generovanou SSL dekrypcí musí být řešena tak, aby byl minimalizován vliv na propustnost a latenci samotné komunikační infrastruktury. S ohledem na charakter provozovaných systémů se požaduje nasazení dvojice externích (FWIPS) a dvojice interních (FWVSS) Next-Generation firewallů v L3 (routed) režimu a v režimu vysoké dostupnosti (active-standby). V případě dvojice interních firewallů jsou požadovány základní funkce NGFW na úrovni aplikačních a identity-based funkcionalit (AVC). Ostatní funkce NGFW nejsou požadovány.

Výčet požadovaných funkcionalit a vlastností pro externí (FWIPS) NGFW:

U této dvojice NGFW bude aktivována funkcionalita IPS a Anti-mallware.

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco FirePower 1150
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	FPR1150 FTD-HA-BUN
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	[redacted]
Typ zařízení	NGFW/NGIPS	ANO
Formát zařízení	Appliance, 1RU	1U
Minimální počet 10/100/1000 BaseT rozhraní dedikovaných pro management	1	1
Minimální počet 10/100/1000 BaseT portů	8	8
Minimální počet SFP portů	2	2
Minimální počet SFP+ portů (10 Gbit)	2	2
EAL4+ certifikace	ANO	ANO [redacted]
Podporovaný počet současně otevřených spojení přes FW	600 000	600000
Rychlost vytváření nových spojení přes FW	28K	28K
Propustnost aplikačního FW (next-gen FW) – (top parametry)	3 Gbps	3GBPS
Propustnost aplikačního FW + IPS (next-gen FW, IPS)	3 Gbps	3GBPS

Podpora L2 (transparentního) módu s podporou NAT a PAT	ANO	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	ANO	ANO
Podpora stateful failover	ANO, active/standby	ANO
Podporovaný počet VLAN	Min. 1024	1024
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Podpora filtrace IPv4, IPv6	Ano	ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	ANO
Podpora inspekce IPv6 provozu	Ano	ANO
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
Podpora NAT64 a DNS64	Ano	ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle	Ano	ANO

uživatelské identity, typu aplikace, apod.		
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Možnost rozšíření o funkce NextGen FW	Ano	ANO
Možnost rozšíření o funkce NextGen IPS	Ano	ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	ANO
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC) *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano	ANO
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	ANO
Funkce VPN		
Maximální počet VPN připojení	alespoň 800	800
Podporované protokoly VPN	SSL/IPSEC (ikev1, ikev2)	ANO
Propustnost IPSEC	Alespoň 1,4 Gbps	1,4
Možnost Autentizace/Autorizace/Accountingu VPN pomocí Externího serveru	LDAP / RADIUS	ANO

Možnost klasifikace VPN provozu a filtrovaní pomocí SGT (Scalable Group Tag) *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Funkce IPS a anti-malware		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	ANO
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	ANO
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podpora různých IPS politik pro různé typy provozu	Ano	ANO
Inspekce pro IPv4 i IPv6	Ano	ANO
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	ANO
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
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	ANO
Podpora aplikace pro psaní zákaznických filtrů	Ano	ANO
Podpora importu komunitních filtrů/signatur Snort	Ano	ANO

IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	ANO
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
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
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	ANO
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	ANO
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	ANO
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	ANO
Možnost definice uživatelské vrstvy politik	Ano	ANO
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	ANO
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	ANO
Podpora aktivní inline ochrany před malware s detekcí známých nebo	Ano	ANO

podezřelých malware nezávislé na aktuálních databázích AV dodavatelů		
Ochrana před malware typu „zero day attack" které nelze detekovat tradičními antiviry	Ano	ANO
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano	ANO
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano	ANO
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano	ANO
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru doddavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	Ano	ANO
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano	ANO
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	ANO
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation"	Ano	ANO

Možnost automatické i manuální klasifikace stanice jako "kritické" se zohledněním v pravidlech, reportech apod.	Ano	ANO
Podpora „remediation" modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	ANO
Otevřené rozhraní pro uživatelsky vytvářené „remediation" moduly	Ano	ANO
Podpora databází reputací adres v Internetu (Security Intelligence) *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Funkce Next-Gen FW		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO
Podpora pasivního monitorování (TAP režim)	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podporovaných aplikací	Min. 3000	4000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO
Filtrace podle typů aplikací webových i ne-webových	Ano	ANO
Filtrace podle reputace serverů	Ano	ANO
SSL inspekce (dekrypce/enkrypce)	Ano	ANO
Security Inteligence database – známé uzly botnet sítí C&C *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod. *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO

Security Inteligence database – známé nebezpečné URL adresy a jmenné domény *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Možnost integrovat vlastní reputační databáze	Ano	ANO
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO
Filtry mohou zohlednit roli a identitu uživatele	Ano	ANO
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	ANO
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO

Výčet požadovaných funkcionalit a vlasností pro interní (FWVSS) NGFW:

Tato dvojice NGFW bude disponovat všemi základními funkcemi Next-Generation Firewallu, mezi které lze zahrnout moderní aplikační a identity-based funkcionality (AVC – application visibility nad control). O jiných (NGFW) funkcionalitách se nyní neuvažuje.

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní uchazeč dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	CISCO FirePower 2130
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede uchazeč hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	FPR2130-NGFW-K9
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	[redacted]

Typ zařízení	NGFW/NGIPS	ANO
Formát zařízení	Appliance, 1RU	1U
Minimální počet 10/100/1000 BaseT rozhraní dedikovaných pro management	1	1
Minimální počet 10/100/1000 BaseT portů	12	12
Minimální počet 10GF portů s volitelným fyzickým rozhraním	4	4
Možnost rozšíření o moduly rozhraní	1	1
EAL4+ certifikace	ANO	ANO [redacted]
Podporovaný počet současně otevřených spojení přes FW	2M	2M
Rychlost vytváření nových spojení přes FW	24K	27K
Propustnost aplikačního FW (next-gen FW) – (top parametry)	4,75 Gb/s	5Gb/s
Propustnost aplikačního FW + IPS (next-gen FW, IPS)	4,75 Gb/s	5Gb/s
Podpora L2 (transparentního) módu s podporou NAT a PAT	ANO	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	ANO	ANO
Podpora stateful failover	ANO, active/standby	ANO
Podporovaný počet VLAN	Min. 1024	ANO
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	ANO

Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Podpora filtrace IPv4, IPv6	Ano	ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	ANO
Podpora inspekce IPv6 provozu	Ano	ANO
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
Podpora NAT64 a DNS64	Ano	ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano	ANO
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ *Zadavatel umožňuje nabídnout rovnocenné řešení.*	Ano	ANO
Možnost rozšíření o funkce NextGen FW	Ano	ANO
Možnost rozšíření o funkce NextGen IPS	Ano	ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	ANO

Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC) *Zadavatel umožňuje nanídnout rovnocenné řešení.*	Ano	ANO
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano	ANO
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	ANO

Funkce Next-Gen FW		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO
Podpora pasivního monitorování (TAP režim)	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podporovaných aplikací	Min. 3000	4000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO
Filtry mohou zohlednit roli a identitu uživatele	Ano	ANO
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury –	Ano	ANO

přepínače, směrovače (např. netflow)		
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO

Požadované vlastnosti a funkcionality centrálního managementu:

V rámci této realizace se požaduje dodání dvou hardwarových managementů pracujících ve vysoké dostupnosti (active-standby). Skrze tento centrální management budou spravovány všechny firewally a jejich Next-Generation funkcionality (Intrusion Prevention System, Security Inteligence, Anti-malware ochranu), tzn. interního i externího NGFW HA páru viz výše. Centrální management musí podporovat případnou správu již nyní provozovaného firewallu Firepower 2110 (VPN koncentrátor provozovaný v HA). Vysoká dostupnost centrálního managementu je zde klíčová z důvodů kritičnosti poskytovaných služeb.

Centralizovaný management musí disponovat funkcemi korelace a automatizace všech událostí z obou dvojic firewallů. Jako příklady můžeme uvést následující: filtrace důležitých událostí, automatické nastavení detekčních jednotek podle typu provozu v síti, zohlednění útoků podle jejich nebezpečnosti v konkrétním prostředí, interakce s externími systémy v případě detekování nebezpečné aktivity v síti, atd.

V oblasti řízení přístupu podle informace o koncovém zařízení musí být možná interakce s externími systémy řídícími přístup do sítě podle kontextu.

Kromě bezpečnostních funkcí musí poskytovat centralizovaný management pohled na kompletní síťovou aktivitu: směr komunikace na úrovni států, objemy datového přenosu podle URL, uživatele, aplikace, typu soborů, apod., viditelnost až do úrovně typů operačních systémů v síti. Dodávaný systém musí umožnit hloubkovou analýzu provozu za účelem získání obsáhlejších informací oproti běžným network monitoring systémům např. na principu netflow. Interní korelační nástroje musí automaticky vyhodnocovat zařízení, která mohla být kompromitována či jsou vzdáleně ovládána. K dispozici musí být flexibilní reporting i možnost napojení na libovolný SIEM. Pro specifické aplikace musí být k dispozici dokumentované API rozhraní pro přístup k informacím a interním databázím centrálního managementu.

Cisco Firepower Management Center 1600

Centrální management pro správu Next-Generation firewallů – obecné funkcionality	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní dodavatel dle nabízeného zařízení**
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	ANO
Přístup ke GUI http/https protokolem	Ano	ANO
Možnost centrální správy při nasazení více firewallů	Ano	ANO

Při centrální správě: možnost sdílených bezpečnostních politik	Ano	ANO
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, *Zadavatel umožňuje nabídnout rovnocenné řešení.* geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	ANO
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	ANO
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano	ANO
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	ANO
Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)	Ano	ANO
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	ANO
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	ANO
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano	ANO
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	ANO
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmorogramu	Ano	ANO

Pro reporty lze definovat template definující formát a obsah reportu	Ano	ANO
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	ANO
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	ANO
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	ANO
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	ANO
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	ANO
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	ANO
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	ANO
Podpora Event Streamer API (eStreamer) pro sdílení informací s externími systémy. Minimálně pro tyto SIEM:	ArcSight	ANO
	BMC Remedy	
	Trustwave	
	NetForensics	
	Novell Sentinel	
	Hawk Network Defense	
	Q1Labs-QRadar	
	Log Rhythm SIEM 2.0	
	LogLogic	
	Splunk	
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	ANO
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	ANO

Podpora řízeného přístupu podle rolí administrátorů	Ano	ANO
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	ANO
Možnost založit pro daný incident „ticket" přímo v prostředí GUI managementu	Ano	ANO
Workflow pro předávání „ticketů" mezi administrátory	Ano	ANO
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu" pro další analýzu	Ano	ANO
Možnost definice politik pro sledování odpovídajících parametrů „zdraví" na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	ANO
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví"	Ano	ANO
Různé politiky pro sledování „zdraví" lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano	ANO
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a musí být schopno zobrazit: — Typ zařízení		ANO
— Operační systém		
— Dodavatel OS		
— Použité síť. protokoly		
— Použité síť. služby		
— Otevřené porty síť. služeb		
— Potenciální zranitelnosti		
Přehled o síťových spojeních má poskytovat minimálně tyto informace: — Čas startu a konce flow		
— Akce (allow, deny,..)		
— Důvod případného blokování		
— Zdroj. a cíl. adresa		
— Vstupní a výstupní zóna		
— Vstupní a výstupní rozhraní		

	Zdroj. a cíl. port		
	Aplikační protokol		
	IPS událost, pokud vznikne		
	Riziková úroveň IPS události		
	Použitá síťová aplikace		
	Rizikovost aplikace		
	„Business impact" aplikace		
	Množství přenesených dat		
Centrální management pro správu Next-Generation firewallů – Technické parametry			
Maximální počet spravovaných zařízení		50	50
Maximální počet IPS událostí		30 milionů	30 milionů
Management rozhraní – alespoň 2x 1 Gbps RJ-45 a 2x SFP+		Ano	ANO
Síťová rozhraní – alespoň 2x 1 Gbps RJ-45		Ano	ANO
Maximum flow rate (flow per second)		5000 fps	5000
Podporuje vysokou dostupnost		Ano	ANO
Redundantní napájecí zdroj		Ano	ANO

Požadované vlastnosti a funkcionality webové proxy:

Dodávané řešení musí umožňovat kontrolu a filtraci veškerého webového provozu minimálně od 100 uživatelů z vnitřní sítě směrem do internetu bude prováděna na technologii s maximální mírou funkcionalit určené k této činnosti s minimalizací vlivu zdržení na koncového uživatele.

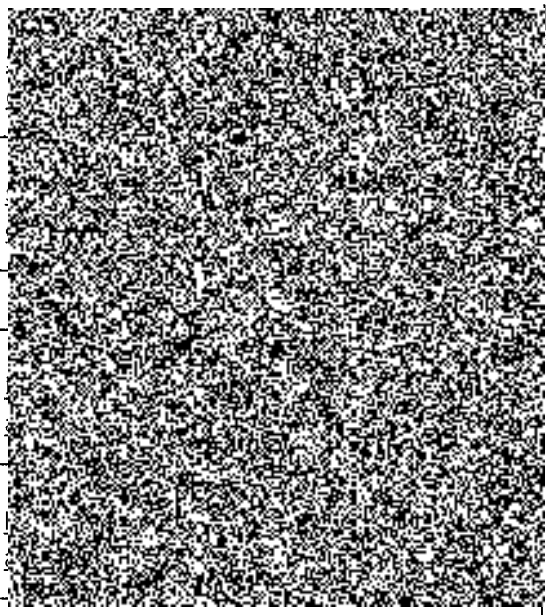
Vzhledem k šifrování velké části webového provozu musí být nasazena kontrola webového provozu s SSL dekrypcí. SSL dekrypce ukončí šifrovanou komunikaci na příslušné technologii a následně musí vytvořit nový šifrovaný kanál na cílové zařízení. Nebezpečné či nežádoucí webové stránky, resp. obsah musí být tímto řešením zablokovány i v případě, že je obsah šifrován. Požaduje se nasazení technologie pro kontrolu webového provozu/obsahu ve virtuálním prostředí provozovatele a to ve vysoké dostupnosti. Bude využita interní virtualizační platforma VMware.

Bez ohledu na dodaný konečný počet virtuálních webových proxy technologií je požadována realizace centrální správy tohoto řešení. Centrální správa musí umožňovat správu veškerých bezpečnostních politik spojených s touto technologií i jednotnou práci nad logy ze všech webových proxy v síti. Z jedno

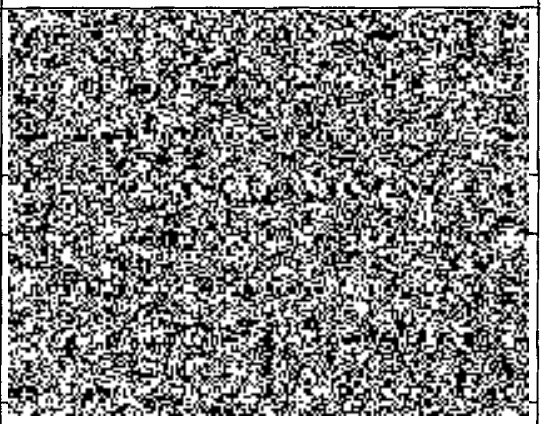
místa musí být možné vyčítat logy o uživatelských aktivitách v rámci webového provozu bez ohledu na to, přes kterou proxy byl učiněn přístup do Internetu.

webova proxy: CISCO WSCA

Požadavky na celkové řešení	**ANO/NE**	**Komentář**
Řešení musí být formou virtuálního appliance do Vmware (rozšíření počtu virtuálních strojů musí být bezplatné)	ANO	WSA-WSS-LIC=
Řešení podporovat centralizovanou konfiguraci pomocí dedikované management appliance	ANO	
Řešení musí podporovat VRRP, nebo jinou podobnou metodu, která umožní vytvořit cluster na virtuální IP adrese	ANO	
Řešení musí podporovat balancování	ANO	
Řešení musí poskytnout podporu na SW, licence a SW po dobu 5 let	ANO	
Řešení musí být jednoduše škálovatelné pro případ rozšíření	ANO	
Řešení musí podporovat navýšení výkonu bez nutnosti zakoupení nové licence	ANO	
Jedno virtuální zařízení musí být schopné zpracovat minimálně 240 požadavků za sekundu při zapnutých všech bezpečnostních funkcích (NTLM ověřování uživatelů, HTTPS dešifrování, antivirus, antimalware, filtrování URL, proxy cache)	ANO	
Malware kontrola a filtrování		
Spyware/Adware/generelní ochrana proti webovým hrozbám (prosíme popište řešení)	ANO	[redacted]
Antivirová ochrana	ANO	
Automatická aktualizace všech antimalware signatur po 5 minutách nebo častěji	ANO	
Podpora současného provozu více antimalware engines přímo na sobě (ne na dalším serveru)	ANO	
AV engines (prosíme vyjmenujte)	ANO	Sophos,Webroot, AMP engine

Ochrana proti phishing útokům (prosíme popište)	ANO	
Automatická aktualizace pravidel na ochranu proti phishing útokům	ANO	
Podpora filtrování URL	ANO	
Minimálně 80 URL kategorií (prosíme vypište seznam)	ANO	
Používané databáze pro URL/web filtrování (prosíme vypište)	ANO	
Vytváření politik per identita/zákazník	ANO	
Definice politik dle časového okna	ANO	
Definice politik dle URL kategorie	ANO	
Definice politik pro cílové URL	ANO	
Definice politik pro cílovou IP adresu/hostname	ANO	
Možnost definice časových a objemových kvót pro uživatele	ANO	
Možnost blokování	ANO	
Možnost pouze monitorovat	ANO	
Možnost zobrazit notifikační stránku při přístupu s možností potvrzení sdělení a vytvoření záznamu v logu	ANO	
Možnost vytvoření vlastních URL kategorií a to i s možností využití regulárních výrazů	ANO	
Kategorizace URL (domén) i vyšších řádů (subdomén)	ANO	
Možnost filtrovat přístup na Webmail	ANO	
Možnost filtrovat přístup na web chat aplikace	ANO	
Dynamická kategorizace nekategorizovaných URL přímo na zařízení	ANO	
Dynamická kategorizace nekategorizovaných URL v cloud výrobce	ANO	
Filtrování na základě web reputace (prosíme popiště reputační technologii)	ANO	

Nastavitelné reputační filtrování na základě hodnoty reputace pro blokování/povolení/skenování obsahu	ANO	
Blokování metody HTTP POST a FTP PUT pomocí metadata (file type, file name, file size)	ANO	
Plnohodnotné a pravdivé skenování obsahu pro detekci typu souboru	ANO	
Skenování na vrstvě TCP pro detekci nakažených stanic s aplikacemi, které komunikují po nestandardních portech	ANO	
Monitorování a blokování malware spojení na všech 65535 portech	ANO	
Monitorování a blokování malware spojení v příchozím i odchozím směru	ANO	
Zařízení musí obsahovat pokročilé funkce proti malware hrozbám	ANO	
Zařízení musí podporovat sandboxing pro neznámé typy souborů	ANO	
Možnost integrace s externími DLP systémy pomocí ICAPS protokolu (RSA, Symantec apod.)	ANO	
Skenování obsahu v komprimovaných souborech a to i včetně rozpoznávání typu souboru (file type)	ANO	
Proxy cache		
Maximální velikost cacheovaného objektu minimálně 1 GB	ANO	
Technologie proxy cache (prosíme specifikujte)	ANO	[redacted]
Implementace v transparentním módu pomocí WCCPv2	ANO	
Implementace v transparentním módu pomocí policy routingu nebo L4 přepínače	ANO	
Implementace jako explicitní proxy	ANO	
Implementace jako explicitní proxy pomocí PAC souboru anebo WPAD	ANO	
Možnost hostování PAC souborů přímo na řešení	ANO	
Podpora více upstream proxy s podmíněným směrováním HTTP provozu	ANO	

Více datových portů pro skenování web provozu	ANO	
Možnost současného provozu řešení v explicitním i transparentním módu	ANO	
Možnost plné modifikace chybových hlášení pro koncové uživatele uvnitř zařízení	ANO	
Kontrola protokolů pro kontrolu		
HTTP	ANO	
HTTPS (dešifrování provozu) s možností selektivního výběru stránek pro dešifrování	ANO	
FTP over HTTP	ANO	
FTP (native)	ANO	
Socks proxy v5	ANO	
Filtrování dílčích elementů web stránek	ANO	
Filtrování konkrétních typů prohlížečů a jejich verzí	ANO	
Blokování Java	ANO	
Blokování ActiveX	ANO	
Detekované typy archivů (prosíme o specifikaci)	ANO	
Detekce vnořených archivů	ANO	
Blokování konkrétních typů souborů (prosíme specifikujte)	ANO	
Detekce a blokování šifrovaných souborů	ANO	
Blokování souborů nad definovanou maximální velikost	ANO	
Monitorování a blokování aplikací P2P, IM, Youtube, Facebook, Flash video na aplikační úrovni (AVC)	ANO	
Možnost omezení šířky pásma pro media streaming provoz (youtube, atd...)	ANO	
Omezování šířky pásma pro video přenosy	ANO	
Ověřování důvěryhodných vydavatelských certifikátů pro HTTPS komunikaci.	ANO	

Granulární rozpoznávání obsahu stránek facebook (tzn. Povolení přístupu na facebook, ale blokování facebook chat, facebook video či facebook games)	ANO	
Ověřování uživatelů		
Autorizace uživatele na základě IP adresy	ANO	
Autorizace uživatele na základě subnetu	ANO	
Ověření uživatele oproti LDAP (LDAPS)	ANO	
Active directory ověření uživatele pomocí NTLMSSP (integrované ověřování Windows) - NTLMv1, NTLMv2, Kerberos	ANO	
Podpora LDAP/Active directory skupin pro přiřazení politik	ANO	
Pro NTLM podpora Windows serverů 2008R2/2012/2016	ANO	
Podpora multidomain v prostředí Windows bez externích agentů	**ANO**	
Možnost integrace s MS AD pomocí externího agenta i bez něj	ANO	
Administrace a management		
HTTPS Management console	ANO	
CLI přístup pomocí SSH	ANO	
Podpora centralizovaného managementu (vytváření konfigurace na jednom místě a poté její automatická distribuce)	ANO	
Ověřování a autorizace administrátorů pomocí RADIUS, LDAP, MS AD	ANO	
Ověřování administrátorů pomocí lokálních účtů	ANO	
Neomezený počet vlastních (administrátorem definovaných) URL kategorií	ANO	
Správa uživatelskými účty s různými právy	ANO	
Napojení do centrálního dohledu pomocí SNMP	ANO	
Podpora centrálního logování pomocí SYSLOG	ANO	
Podpora centrálního logování pomocí kopírování logů skrze FTP a SCP	ANO	

Systém a podpora (v případě realizace řešení více appliance se uvedené požadavky vztahují na každou z nich)		
řešení musí mít formu virtual appliance s vlastním proprietárním operačním systémem	ANO	
Podpora pro tři (3) virtuální rozhraní v rámci virtuální platformy pro služby web security	ANO	
Poskytovaná podpora přímo od výrobce	ANO	
Podpora výrobce formou email, telefon, web	ANO	
Přístup na portál podpory výrobce a znalostní báze	ANO	
Plná podpora hardware po dobu trvání kontraktu podpory	ANO	
Reporting		
GUI rozhraní pro účely administrace a prohlížení reportů	ANO	
Možnost vlastního nastavení reportu	ANO	
Možnost detailního prohlížení reportů pro každého uživatele a jeho aktivit pro účely analýzy	ANO	
Export reportů a plánování jejich pravidelného zasílání	ANO	
Zobrazení podezřelých aktivit pro každého uživatele	ANO	
Top-N reporty pro: Top uživatele, top URL, top URL kategorie, top malware, používání web aplikací	ANO	
Možnost ukládání reportu v PDF a CSV formátu	ANO	
Možnost rozšířený reportingu pomocí externího zařízení nebo softwaru, který umožní vysokou úroveň modifikace a úpravu reportů dle aktuálních pozažadavků	ANO	
Funkce Web Security Management a Reporting		
Centralizovaná replikace konfigurace na více web security zařízení	ANO	
Skupinování web security zařízení do skupin	ANO	
Možnost delegace práv pro konfigurování pouze konkrétní politiky konkrétnímu administrátorovi	ANO	
Správa web security zařízení s různými verzemi OS	ANO	
Možnost schovat ostatní politiky pro delegovaného administrátora	ANO	

Možnost zobrazit ostatní politiky pouze pro čtení pro delegovaného administrátora	ANO	
Možnost plánování update politik na konkrétní čas	ANO	
Centralizovaná kolekce dat od více web security zařízení	ANO	
Vytváření konsolidovaných reportů z dat od více web security zařízení	ANO	
Možnost sledování a dohledávání konkrétní transakce přes více web security zařízení pomocí jednoho GUI rozhraní	ANO	
Vygenerování reportu on-demand o aktuální aktivitě daného uživatele	ANO	
Historické ukládání reportů a dostupnosti reportovaných dat	ANO	
Plánované reporty pro doručení	ANO	

Požadované vlastnosti a funkcionality ochrany mobilních zařízení (teleworkers):

Ochrana Webových aktivit přes DNS službu

Požadujeme dodat řešení, které zajistí prevenci, detekci a blokaci nežádoucí komunikace na kompromitované DNS či IP adresy v Internetu. Bezpečnostní platforma se předpokládá na cloudovém řešení, kdy bude provedeno porovnání se záznamy v databázích, kde se ověří validita a riskové skóre cílové adresy a také souvztažnosti k případným provozovatelům botnet sítí. Toto řešení bude nasazeno především na zařízeních interních uživatelů, kteří využívají mobilní zařízení i mimo zabezpečený vnitřní perimetr sítě. Co do počtu se jedná o 40 zařízení.

Nasazením této technologie se především sleduje zajištění stejné bezpečnostní politiky na mobilní zařízení uvnitř i mimo vnitřní síť.

Ochrana Webových aktivit přes DNS službu

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní dodavatel dle nabízeného zařízení**
Výrobce technologie	Uvedení výrobce	Cisco Umbrella DNS security
Cloudová služba využívající ANYCAST routing, s podporou globálního load-balacning-u a transparentního fail-over	Ano	ANO
Řešení pracuje s více data centry po celém světě (taky v rámci EU) pro zabezpečení 100% dostupnosti	Ano	ANO
Žádná přidaná odezva pro koncového uživatele	Ano	ANO

Jednoduché nasazení jenom pomocí změny DNS nebo DHCP nastavení globální IP adresy cloudové služby	Ano	ANO
Řešení nevyžaduje nasazení žádného hardwarového zařízení na straně uživatele	Ano	ANO
Musí chránit každé zařízení v síti včetně IoT a neřízených zařízení	Ano	ANO
Podpora roamingových služeb pro uživatele mimo interní síť	Ano	ANO
Nutná integrace s řešením „Vzdálený VPN přístup pro mobilní uživatele a jednotný klient"formou rozšířeného modulu VPN klienta pro roamingové uživatele bez potřeby dalšího softwaru – případná potřebná licence musí být součástí řešení	Ano	ANO
VPN klient modul, nebo samostatný softwarový klient se musí aktualizovat automaticky prostřednictvím cloudové infrastruktury	Ano	ANO
Ochrana roamingového uživatele i v čase kdy není aktivně připojen přes VPN	Ano	ANO
Možná integrace na úrovni směrovače nebo wireless kontrolérů	Ano	ANO
Podpora statistických metod a strojového učení k detekci vznikajících hrozeb	Ano	ANO
Blokace spojení s nebezpečnými destinacemi na úrovni DNS a IP vrstev	Ano	ANO
Znalostní databáze nebezpečných destinací na úrovni DNS	Min. 7 mil destinací	ANO
Blokace škodlivých URL na úrovni HTTP/S s podporou integrace reputačních databází třetích stran	Ano	ANO
Real-time anti-malware sken pro blokaci stahování souborů ze škodlivých domén na základě jejich reputace	Ano	ANO
Proaktivní analýza průtokových dat pro identifikaci vzorků, odhalování anomálií a vytváření statistických modelů pro automatické odhalení dalších hrozeb	Ano	ANO

Automatické vytváření skóre a klasifikace dat za účelem zjištění anomálií a odhalení známých a vznikajících hrozeb	Ano	ANO
Real-time korelace toku dat s historickým provozem služby	Ano	ANO
Možnost integrace s uživatelskou databází – Active Directory – případná potřebná úroveň licence musí být součástí řešení	Ano	ANO
Možnost přizpůsobení notifikace o blokované stránce vlastním textem	Ano	ANO
Vytváření whitelistů/blacklistů domén	Ano	ANO
Možnost bypassu block page bezpečnostním kódem nebo pro konkrétní uživatele	Ano	ANO
Blokace škodlivých domén na úrovni IP adresy, bez DNS překladu	Ano	ANO
Export logů do Amazon S3 služby	Ano	ANO
Nástroj na testování politik před jejich reálným nasazením	Ano	ANO
Možnost připojení na SIEM	Ano	ANO
Modul pro designování a plánování reportů, sledování návštěvnosti domén, aktivity uživatelů, četnosti bloků v korelaci s globálním provozem	Ano	ANO
Licencování na základě počtu uživatelů nebo počtu access pointů	Ano	ANO
Možnost správy několika oddělených síťových domén v rámci jedné web GUI management konzole	Ano	ANO
Možnost dvoufázové autentizace vůči management konzoli nebo pomocí SAML tokenu z SSO služby třetí strany	Ano	ANO

Anti-malware zabezpečení

Požaduje se dodat takové řešení pro mobilní zařízení interních uživatelů, aby i při práci mimo perimetr interní sítě byla zajištěna obdobná úroveň bezpečnosti, jako při práci uvnitř sítě.

Je požadováno dodání řešení pro zajištění komplexní bezpečnosti pro 40 zařízení (enpointů), tzn. antivirové řešení vč. možnosti heuristické analýzy a funkce detekce/prevence malware (reputační, behaviorální filtry, machine learning, dynamická analýza souboru - sandbox, fuzzy finger-printing). Kromě detekce a ochrany proti malware se požaduje funkcionalita retrospektivy z důvodu trasování, jakým vektorem, odkud a kdy se malware na stanici objevil.

Anti-malware zabezpečení Cisco AMP endpoint

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní dodavatel dle nabízeného zařízení**
Software na koncové stanici musí být menší než 100 MB a musí podporovat manuální a / nebo bezobslužnou instalaci	CISCO AMP endpoint	[redacted]
Software pro koncové stanice musí být snadno nasaditelný a musí podporovat (nejen) nasazení pomocí nástrojů pro správu systémů také 3. stran	CISCO AMP endpoint	ANO
Software musí být podporován na následujících platformách:	CISCO AMP endpoint	ANO
- Windows	CISCO AMP endpoint	ANO
- Mac	CISCO AMP endpoint	ANO
- Linux	CISCO AMP endpoint	ANO
- Android	CISCO AMP endpoint	ANO
- Virtuální zařízení	CISCO AMP endpoint	ANO

Analýza hlavní příčiny na podezřelých koncových stanicích musí poskytovat min. následující funkce:		
- Sekvenční a chronologické stopy událostí s detaily, včetně hostitele, uživatelského jména, IP adresy a klientské aplikace	CISCO AMP endpoint	ANO
- Podrobnosti by měly zdůrazňovat, který soubor, proces, nebo služby byly ovlivněny	CISCO AMP endpoint	ANO
Navržený software pro koncové body musí podporovat sledování podezřelých souborů (malware) a poskytnout vizualizaci na úrovni sítě: postižené uživatele, systémy, Patient Zero Day Zero (způsob a místo jakým hrozba pronikla do sítě)	CISCO AMP endpoint	ANO
Navrhované řešení musí podporovat sledování chování souboru, aktivity jednotlivých procesů a umí automaticky generovat výstrahy při prvních známkách škodlivého chování	CISCO AMP endpoint	ANO
Navrhovaný systém musí podporovat průběžné a neustálé monitorování souborů pro retrospektivní náhled detekce /	CISCO AMP endpoint	ANO

blokování hrozby (malware)		
Řešení musí umět identifikovat zranitelný software a chyby zabezpečení na koncovém bodu	CISCO AMP endpoint	ANO
Navrhovaný systém musí podporovat úplnou analýzu souborů v zabezpečené karanténě (sandbox) poskytující podrobnou zprávu o podezřelém chování souboru malware	CISCO AMP endpoint	ANO
Součástí řešení musí být přístup k dashboardu sandboxové analýzy, pokud se nejedná o primární dashboard řešení	CISCO AMP endpoint	ANO
Navrhované řešení umožňuje vyšetřování zabezpečení pomocí pokročilé detekce a reakce koncových bodů (EDR)	CISCO AMP endpoint	ANO
Navrhovaný software pro koncové body musí být schopen blokovat CnC komunikaci, Sniffer/Dropper aktivity a obsah pro šíření škodlivého kódu	CISCO AMP endpoint	ANO
Reakce na událost a její náprava na koncových musí min. obsahovat:		
- Sledování a zachytávání souborů s možností vyhledat škodlivé soubory na	CISCO AMP endpoint	ANO

podezřelých koncových bodech		
- Blokování souborů, procesů nebo služeb, které vykazují škodlivé chování	CISCO AMP endpoint	ANO
- Detekce Dropper aktivit a blokování stahování přes URL / web stránky	CISCO AMP endpoint	ANO
- Možnost odeslat podezřelé škodlivé soubory pro další analýzu	CISCO AMP endpoint	ANO

Centrální incident response konzole

Z důvodu urychlení a zjednodušení reakce na incidenty se požaduje dodání centrální konzoly pro reakce na síťové bezpečnostní incidenty, která propojí veškeré dodávané technologie (antimalware ochranu několika úrovních, perimetrové a interní Next-Generation Firewally, Webové proxy i mobilní zařízení). Tato centrální console musí automaticky korelovat události s cílem objasnit chování malwaru, resp. zajistit retrospektivu (kudy, přes jaké zařízení, kdy se do sítě malware dostal a jak se vyvíjelo jeho chování v čase).

Centrální incident response konzole

Požadované vlastnosti přepínačů pro připojení externích konektivit

SWITCHe

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní dodavatel dle nabízeného zařízení**
Výrobce zařízení	Uvedení výrobce	Cisco Catalyst **C9200L-24T-4G**
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-24T-4G
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	[redacted]
Typ přepínače	L2/L3 přepínač	L2/L3
Formát přepínače	Stohovatelný	ANO
Minimální počet zařízení ve stohu	8	8
Minimální kapacita sběrnice stohu	80 Gb/s	80Gb/s
Minimální kapacita přepínání	200 Gb/s	208Gb/s
Minimální paketová kapacita	95 Mp/s	95,23 Mp/s
Stateful Switch Over v rámci stohu	ANO	ANO
Velikost zařízení 1RU	ANO	ANO
Min. velikost sdíleného systémového paketového bufferu	6 MB	6MB

Redundatní ventilátory	ANO	ANO
Možnost instalovat interní redundantní napájecí zdroj	ANO	ANO
Interní redundantní napájecí zdroj požadován	ANO	ANO
Počet dedikovaných stohovacích portů	2	2
Možnost stohování přes dedikované porty, bez snížení počtu použitelných ethernetových portů	ANO	ANO
Stohování požadováno	ANO	ANO
Datový stohovací kabel požadován (0.5m/1m/3m)	ANO	ANO
Počet portů 10/100/1000 Base-TX	24	24
Minimálně 4x Uplinkové porty s volitelným rozhraním SFP+	ANO	24
Velikost MAC address tabulky	16000	16000
Min. počet IPv4 routes	3000	3000
Min. počet IPv6 routes	1500	1500
Min. počet konfigurovatelných security ACL	1500	1500
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	32	32
IEEE 802.1Q	ANO	ANO
Minimální počet aktivních VLAN	1000	4096
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 ju MBo rámců (min. 9198 bytes)	ANO	ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	ANO
Směrování protokolů IPv4 a IPv6 v hardware	ANO	ANO

RIP, EIGRP Stub, OSPFv2; OSPFv3 - minimálně 1000 Routes	ANO	ANO
OSPFv2; OSPFv3 (povýšením firmware)	ANO	ANO
FIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) (povýšením firmware)	ANO	ANO
ISIS (povýšením firmware)	ANO	ANO
IP Multicast (PIM SSM, PIM SM) (povýšením firmware)	ANO	ANO
HSRP (povýšením firmware)	ANO	ANO
VRRP	ANO	ANO
Reverse path check (uRPF) pro IPv4 i IPv6 (povýšením firmware)	ANO	ANO
IGMPv2, IGMPv3	ANO	ANO
IGMP snooping	ANO	ANO
MLD snooping	ANO	ANO
Minimální počet HW QoS front	8	8
QoS classification – ACL, DSCP, CoS based	ANO	ANO
QoS marking - DSCP, CoS	ANO	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	ANO
QoS Policing	ANO	ANO
QoS-Hierarchical QoS	ANO, min. 2 úrovně	ANO
IPv6 First Hop Security (RA guard, DHCPv6	ANO	ANO

snooping, IPv6 source guard)		
Možnost definovat povolené MAC adresy na portu	ANO	ANO
PACL, VACL	ANO	ANO
IEEE 802.1ae na uplink portech	ANO	ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	ANO
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
IEEE 802.3az	ANO	ANO
Automatická aplikace specifické konfigurace pro dané zařízení po	ANO	ANO

detekci jeho připojení na portu		
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 pomocí "Blue Beacon" mechanismu	ANO	ANO
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní události 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
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
NTPv3 server	ANO	ANO

Příloha č. 2 – Cenová kalkulace

Položka	Typ	Počet	Cena bez DPH v Kč	Sazba DPH	DPH v Kč	Cena včetně DPH v Kč
CISCO FirePower 1150	HW	2	855 060,00	21 %	179 562,60	1 034 622,60
CISCO FirePower 2130	HW	2	288 000,00	21 %	60 480,00	348 480,00
CISCO Management Center 1600	HW	2	430 000,00	21 %	90 300,00	520 300,00
Cisco Threat Defense Threat and Malware License	Licence	2	315 010,00	21 %	66 152,10	381 162,10
Webová proxy CISCO WSCA 50 users	Licence	2	455 100,00	21 %	95 571,00	550 671,00
Cisco Umbrella DNS security 20 users	Licence	2	211 200,00	21 %	44 352,00	255 552,00
Anti-malware zabezpečení Cisco AMP endpoint 20 users	Licence	2	234 107,00	21 %	49 162,47	283 269,47
Cisco Catalyst C9200L-24T-4G	HW	2	250 000,00	21 %	52 500,00	302 500,00
Práce			857 565,00	21 %	180 088,65	1 037 653,65
Doplňující prvky pro integraci nového zařízení do stávající infrastruktury	HW	10	41 681,00	21 %	8 753,01	50 434,01
Celkem:			3 937 723,00	21 %	826 921,83	4 764 644,83