SML/2018/254

KUPNÍ SMLOUVA

č.

č.j. ČÚZK-01748/2019-24

---

uzavřená dle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „Smlouva")

1.
GC System a.s.
se sídlem Špitálka 41, č. p. 113, 602 00 Brno
zastoupen: [redacted], předsedou představenstva a ředitelem společnosti
IČO: 64509826
DIČ: CZ64509826 zapsána v Obchodním rejstříku vedeným Krajským soudem v Brně, oddíl B, vložka 1927

a

ALEF NULA,a.s.
IČO: 61858579
se sídlem Pernerova 691/42, Karlín, 186 00 Praha 8
vedená u Městského soudu v Praze, oddíl B, vložka 2727
zastoupena [redacted], předsedou představenstva

(dále obě společnosti dohromady jen „Dodavatel")

2. Česká republika – Český úřad zeměměřický a katastrální
se sídlem Pod sídlištěm 1800/9, Kobylisy, 182 11 Praha 8
IČO: 00025712
tel.: 0284041207
fax: 0284041204
e-mail: [redacted]@cuzk.cz
jejímž jménem jedná Ing. Karel Štencel, místopředseda
(dále jen „Objednatel")

I.

Předmět smlouvy

1. Předmět plnění této Smlouvy je dodání komponent a služeb specifikovaných blíže v příloze 1 této Smlouvy (dále jen „plnění").
2. Plnění bude Dodavatelem poskytnuto způsobem a v rozsahu stanoveném v této Smlouvě, jejích přílohách, zadávací dokumentaci k veřejné zakázce „Obnova síťové infrastruktury ČÚZK" a nabídce Dodavatele předložené v rámci této veřejné zakázky. Plnění bude Dodavatel provádět na profesionální úrovni v kvalitě odpovídající všeobecně uznávaným standardům pro daný okruh činností.
3. Dodavatel deklaruje, že osoby a/nebo případně poddodavatelé, jejichž odbornou kvalifikací bylo prokázáno v jeho nabídce na veřejnou zakázku splnění technických kvalifikačních předpokladů, budou skutečně zapojeny do plnění předmětu Smlouvy minimálně do doby akceptace plnění. V případě nutné změny těchto osob a/nebo poddodavatelů z důvodů mimo vůli Dodavatele musí Dodavatel doložit splnění srovnatelných kvalifikačních předpokladů pro nové osoby a/nebo poddodavatele. Po dobu, kdy Dodavatel neplní tento svůj závazek, je v prodlení s poskytováním plnění dle této Smlouvy a Objednatel má právo požadovat slevu z ceny plnění ve výši 0,2 % z celkové ceny plnění za každý den takového prodlení.
4. Obsahem tohoto závazkového vztahu jsou všechny podmínky, práva a povinnosti stanovené v zadávací dokumentaci a jejích přílohách a nabídce Dodavatele i v případě, že nejsou touto Smlouvou výslovně uvedeny. Smluvní strany prohlašují, že tuto Smlouvu, jakož i jednotlivá práva a povinnosti z ní vyplývající, budou vykládat v souladu se zadávací dokumentací, všemi podmínkami stanovenými v rámci zadávacího řízení zadání veřejné zakázky a nabídkou Dodavatele předložené v rámci tohoto zadávacího řízení.
5. Veškeré odchylky od specifikace předmětu plnění podle předchozích bodů mohou být prováděny Dodavatelem pouze tehdy, budou-li písemně odsouhlaseny Objednatelem. Jestliže Dodavatel provede práce a jiná plnění nad tento rámec odsouhlasený Objednatelem, nemá nárok na jejich zaplacení.
6. Dodavatel poskytne na vlastní náklady právní servis včetně zastoupení Objednatele v případě, že budou vůči Objednateli vzneseny jakékoli nároky před soudem nebo mimo soud, pokud se tyto nároky vztahují na porušení duševního vlastnictví, jako například patentových a autorských práv a obchodních značek, v důsledku používání Produktu dodaného Objednatelem dle této Smlouvy. Dodavatel uhradí veškeré škody a náklady, které bude Objednatel povinen v důsledku výše uvedeného uhradit. Toto zastupování bude poskytnuto v případě, že Dodavatel bude neprodleně písemně informován Objednatelem o nároku uplatněném třetí stranou a budou mu ze strany Objednatele poskytnuty potřebné informace a plná moc k zastupování Objednatele v řízení o daném nároku.

II.
Kupní cena

1. Smluvní strany se dohodly na kupní ceně, která činí 57 197 949,- Kč bez DPH, 69 209 519,- Kč s DPH. Rozpad ceny na jednotlivé položky:

Cenová tabulka č. 1 – první fáze implementace

Číslo řádku	Plnění	Cena za jeden kus v Kč bez DPH (včetně 6-ti letého záručního servisu)	Celková cena v Kč bez DPH	Celková cena v Kč s DPH
1	Loadbalancing – 4 ks loadbalanceru	3 367 675 Kč	13 470 700 Kč	16 299 547 Kč
2	NGFW – 4ks NextGeneration FireWall	3 200 768 Kč	12 803 072 Kč	15 491 717 Kč
3	Monitoring NetFlow (cena za řešení)	----------	4 909 303 Kč	5 940 257 Kč
4	Jednotný management pro šifrátory a DC switching – část pro 1. fázi (cena za řešení)	----------	370 407 Kč	448 192 Kč
5	Analýza řešení propojení se stávající infrastrukturou a ostatní implementační práce fáze 1 (jako celek)	----------	1 734 000 Kč	2 098 140 Kč
6	Dokumentace k první fázi	----------	918 000 Kč	1 110 780 Kč
7	Školení – 16 hod/5 uživatelů	----------	34 000 Kč	41 140 Kč
8	**Celková nabídková cena za první fázi implementace**		34 239 482 Kč	41 429 774 Kč

Tabulka 1a Rozpad ceny za Jednotný management pro šifrátory a DC switching – ceny licencí

Číslo řádku	Plnění	Cena za jeden kus v Kč bez DPH (včetně 6-ti letého záručního servisu)	Celková cena v Kč bez DPH	Celková cena v Kč s DPH
1	Serverové licence (počet a cena)	0 Kč	0 Kč	0 Kč
2	Device licence (počet a cena)	3 704 Kč	370 407 Kč	448 192 Kč
3	Případné další náklady (bez impl. prací)	----------	0 Kč	0 Kč
4	**Celková nabídková cena za Jednotný management v 1. fázi implementace**		370 407 Kč	448 192 Kč

Tabulka 1b Rozpad ceny za Monitoring NetFlow a 802.1x- ceny licencí

Číslo řádku	Plnění	DPH (včetně 6-ti leté záručního servisu)	Celková cena v Kč bez DPH	Celková cena v Kč s DPH
1	Serverové licence (počet a cena)	1 245 208,37	2 490 416,73	3 013 404 Kč
2	Device licence (počet a cena)	159,80	159 800,00	193 358 Kč
3	Uživatelská licence	0	0	0 Kč
4	Případné další náklady (bez impl. prací)	----------	0	0 Kč
5	**Celková nabídková cena za Monitoring NetFlow + 802.1x**		2 650 216,73	3 206 762 Kč

Cenová tabulka č. 2 – druhá fáze implementace

Číslo řádku	Plnění	Cena za jeden kus v Kč bez DPH (včetně 6-ti letého záručního servisu)	Celková cena v Kč bez DPH	Celková v Kč s DPH
1	DC switching – 4 ks datacentrového přepínače	2 395 851 Kč	9 583 403 Kč	11 595 918 Kč
2	Out of band mangement switche – 2ks	68 588 Kč	137 176 Kč	165 982 Kč
3	DWDM – 4ks DWDM zařízení	2 696 129 Kč	10 784 514 Kč	13 049 262 Kč
4	Jednotný management pro DC switching – část pro 2. fázi implementace (cena za řešení)	----------	413 374 Kč	500 183 Kč
5	Cena za implementační práce ve druhé fázi (jako celek)	----------	1 122 000 Kč	1 357 620 Kč
6	Dokumentace k druhé fázi implementace	----------	629 000 Kč	761 090 Kč
7	Školení – 16 hod/5 uživatelů	----------	34 000 Kč	41 140 Kč
8	**Celková nabídková cena za druhou fázi implementace**		22 703 467 Kč	27 471 195 Kč

Tabulka 2. a Rozpad ceny za Jednotný management pro DC switching druhá fáze implementace

Číslo řádku	Plnění	Cena za jeden kus v Kč bez DPH/ks včetně 6-ti letého podpory	Celková cena za všechny ks se záručním servisem v Kč bez DPH	Celková cena za všechny ks se záručním servisem v Kč s DPH
1	Serverové licence (počet a cena)	48 652,99	48 652,99	58 870 Kč
2	Device licence (počet a cena)	91 180,29	364 721,18	441 313 Kč
4	Případné další náklady (bez impl. prací)	----------	0	0 Kč
5	**Celková nabídková cena za Jednotný management v 2. fázi implementace**		413 374,17	500 183 Kč

Cenová tabulka č. 3 – Nabídková cena 15 MD

Číslo řádku	Plnění	Cena za 1 MD bez DPH	Cena celkem bez DPH	Cena celkem s DPH
1	**Vícepráce v rozsahu 15 MD**	17 000 Kč	255 000 Kč	308 550 Kč

Cenová tabulka č. 4 – Celková nabídková cena

Číslo řádku	Plnění	Cena v Kč bez DPH	Cena v Kč s DPH
1	Celá první fáze implementace	34 239 482 Kč	41 429 774 Kč
2	Celá druhá fáze implementace	22 703 467 Kč	27 471 195 Kč
3	Vícepráce v rozsahu 15 MD	255 000 Kč	308 550 Kč
4	**Celková nabídková cena za plnění celé VZ**	57 197 949 Kč	69 209 519 Kč

2. Ceny nabídnuté Dodavatelem jsou cenami nejvýše přípustnými, které není možno překročit. Ceny zahrnují veškeré náklady Dodavatele nutné pro řádnou realizaci plnění. K ceně nabídnuté Dodavatelem bude připočtena DPH ve výši stanovené právními předpisy v době zdanitelného plnění.

III.

Platební podmínky

1. Cena plnění zahrnuje veškeré náklady Dodavatele nutné k poskytnutí plnění, jakož i veškeré náklady související. Dodavatel prohlašuje, že před podpisem této Smlouvy, důkladně prošel zadávací dokumentaci a všechny případně poskytnutá vysvětlení, zvážil všechny varianty možného způsobu plnění zakázky a na základě těchto informací stanovil cenu plnění uvedenou do nabídky. Tato cena je maximální a nepřekročitelná a Dodavatel je povinen za tuto cenu plnění dokončit tak, aby bylo dosaženo účelu a předmětu této Smlouvy, a to i v případě, že by se v průběhu plnění Smlouvy zjistilo, že ke splnění účelu a předmětu této Smlouvy je nutné vynaložit další náklady nebo zvolit jiné postupy.
2. Smluvní strany se dohodly na bezhotovostním placení na účet Dodavatele dle pravidel uvedených v následujících odstavcích.
3. Cena plnění bude uhrazena Dodavateli postupně, nejdříve její první část ceny na základě akceptace první fáze implementace a následně druhá část ceny po celkové akceptaci plnění. Fakturované částky budou odpovídat cenám za jednotlivé vrstvy uvedené v cenové specifikaci. Objednatel požaduje fakturaci druhé části ceny plnění v roce 2020.
4. Vystavená faktura bude mít náležitosti stanovené zákonem o DPH č. 235/2004 Sb., v platném znění a termín splatnosti 21 dnů po doručení Objednateli. Povinnost zaplatit je splněna dnem odepsání příslušné finanční částky z bankovního účtu Objednatele na účet Dodavatele uvedený v záhlaví této Smlouvy, není-li smluvními stranami sjednáno jinak.
5. Nebude-li vystavená faktura obsahovat náležitosti uvedené v předchozích ustanoveních nebo bude chybně vyúčtována cena, bude taková faktura do data splatnosti Dodavateli vrácena k doplnění scházejících údajů nebo k opravě nesprávných údajů. Dodavatel provede opravu vystavením nové faktury s novou dobou splatnosti, která nesmí být co do počtu dnů kratší než doba splatnosti původní faktury. Bude-li vadná faktura vrácena, přestává běžet původní doba splatnosti. V takovém případě nedojde k prodlení s

placením. Celá doba splatnosti běží znovu ode dne doručení nově vystavené faktury na konkrétní fakturační místo.

IV.

Smluvní sankce

1. V případě prodlení Objednatele s úhradou plateb sjednaných v této Smlouvě, je Dodavatel po Objednateli oprávněn požadovat uhrazení smluvní pokuty ve výši 0,05 % z dlužné částky za každý započatý den prodlení.
2. V případě prodlení s předáním plnění nebo jeho součásti má Objednatel právo požadovat po Dodavateli slevu z ceny ve výši 0,5% z ceny plnění za každý započatý den prodlení a nedodané zařízení.
3. V případě nesplnění povinnosti Dodavatele zajistit připojení k helpdesku ČÚZK má Objednatel právo požadovat po Dodavateli smluvní pokutu ve výši 5 000 Kč za každý započatý pracovní den nesplnění této povinnosti.
4. V případě nesplnění garantované úrovně servisu ze strany Dodavatele má Objednatel právo požadovat po Dodavateli slevu z ceny (případně smluvní pokutu, pokud už nebude následovat další fakturace) ve výši 10 000 Kč za každý i započatý pracovní den nedodržení fix-time opravy.
5. Za porušení povinnosti mlčenlivosti je porušující smluvní strana povinna uhradit druhé straně smluvní pokutu ve výši 100 000 Kč, a to za každý jednotlivý případ porušení povinnosti.
6. Sleva z ceny bude poskytnuta v rámci fakturace bezprostředně následující po porušení povinnosti Dodavatele.
7. Vznikem nároku na uplatnění slevy z ceny či smluvní pokuty není dotčen nárok smluvní strany na náhradu vzniklé škody přesahující poskytnutou slevu z ceny či smluvní pokutu.
8. Poskytnutí slevy z ceny či smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.
9. Každá ze smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje sleva z ceny či smluvní pokuta, a to v celém rozsahu. Odstoupením od Smlouvy nárok Objednatele na slevu z ceny či smluvní pokutu nezaniká.

V.

Seznam příloh

1. Příloha č. 1 – Podrobná specifikace předmětu smlouvy a servisní parametry

VI.

Mlčenlivost

1. Smluvní strany se zavazují, že během plnění Smlouvy i po jejím ukončení budou chránit důvěrné informace druhé strany tak, jako chrání svoje vlastní informace stejné důležitosti a zachovávat mlčenlivost o všech důvěrných informacích, o kterých se dozví od druhé strany v souvislosti s plněním Smlouvy. Objednatel považuje mimo jiné za důvěrné veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se technické infrastruktury, které nejsou obecně známé, a dále takové informace, které jím budou jako důvěrné výslovně označeny. Za porušení povinnosti mlčenlivosti se považuje

i nezajištění vymazání dat z pevného disku při servisním zásahu a jejich zpřístupnění byť nezaviněné, třetí osobě.

VII.

Odstoupení od smlouvy

1. Strany jsou oprávněny od Smlouvy odstoupit pouze v případě závažného porušení smluvní nebo zákonné povinnosti protistranou. Odstoupení od Smlouvy nabývá účinnosti písemným doručením oznámení o odstoupení druhé straně.
2. Za závažné porušení Smlouvy ze strany Dodavatele se považuje zejména zpoždění s řádným plněním dle Smlouvy (zejména pozdní dodání) delším než 7 pracovních dní. Za závažné porušení Smlouvy se také považují případy, kdy se v průběhu plnění první fáze implementace vyskytnou závažné problémy s funkčností anebo bezpečnostního rázu. Objednatel bude v takovém případě akceptovat pouze vyhovující část řešení a uhradí cenu takové části řešení dle cen uvedených v cenové tabulce.
3. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněného nároku na zaplacení smluvních pokut resp. poskytnutí slev z cen.
4. Ukončením účinnosti této Smlouvy nejsou dotčena ustanovení Smlouvy o ochraně informací a ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.

VIII

Doba a místo plnění akceptace

1. Dodavatel zahájí dodávky zařízení a instalaci 28 dní po podpisu Smlouvy a dokončí první fázi implementace do 150-ti dní od zahájení a druhou fázi implementace zahájí po 28 denním bezproblémovém provozu první fáze a dokončí ji do 150 dní od jejího zahájení. V případě výskytů problémů ve zkušebním provozu první fáze Objednatel posoudí jejich závažnost a rozhodne, zda prodlouží zkušení provoz o dalších 28 dní (aniž by došlo k prodlení Dodavatele s plněním dle Smlouvy) nebo využije svého práva a od Smlouvy odstoupí, aniž by došlo k realizaci druhé fáze implementace.
2. Záruční servis bude Dodavatelem poskytován po dobu 72 měsíců od celkové akceptace plnění.
3. Dodavatel dodá Objednateli nejpozději do 15 dnů po podpisu této Smlouvy návrh harmonogramu dodávek a instalací první fáze implementace k připomínkám a vzájemnému odsouhlasení.
4. Dodavatel odpovídá za to, že poskytnuté plnění bude ke dni celkové akceptace a splňovat funkční specifikaci stanovenou zadávacími podmínkami, jeho nabídkou do zadávacího řízení a touto Smlouvou a bude implementovatelné a provozuschopné v prostředí Objednatele. Dále Dodavatel odpovídá za to, že po akceptaci jednotlivých fází implementace budou vrstvy v této fázi realizované splňovat funkční specifikaci stanovenou zadávacími podmínkami, jeho nabídkou do zadávacího řízení a touto Smlouvou a budou provozuschopné v prostředí Objednatele. Vadou se rozumí rozpor mezi skutečnými funkčními vlastnostmi poskytnutého plnění a funkčními vlastnostmi, které jsou stanoveny ve výše uvedených dokumentech. Za vadu se považuje i skutečnost, že funkční vlastnosti poskytnutého plnění neodpovídají povinným funkčním

vlastnostem, jak vyplývají z technických norem, pokud se takové technické normy na plnění vztahují a jsou vůči němu závazné. Za vadu se dále považují i právní vady plnění.

5. Místem plnění je sídlo ČÚZK a primární datové centrum, které je umístěno v Kongresovém centru Praha, 5. května 1640/65, 140 00 Praha 4.

IX

Závěrečná ujednání.

1. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných za každou smluvní stranu osobou nebo osobami oprávněnými jednat jménem smluvních stran.
2. Spory vyplývající z této Smlouvy nebo vzniklé v souvislosti s ní nebo vzniklé v souvislosti s plněním mezi Objednatelem a Dodavatelem budou řešeny především dohodou. Pokud k dohodě nedojde, budou spory projednávány před soudy České republiky. V případě řešení sporů před soudem si smluvní strany sjednávají místní příslušnost prvoinstančního soudu podle místa sídla Objednatele.
3. Smluvní strany berou na vědomí, že tato Smlouva podléhá zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a účinnosti nabyde nejdříve dnem zveřejnění smlouvy v tomto registru.
4. Obě společnosti na straně Dodavatele deklarují, že budou vůči Objednateli a třetím osobám z jakýchkoliv právních vztahů vzniklých v souvislosti se Smlouvou (veřejnou zakázkou) zavázáni společně a nerozdílně, a to po celou dobu plnění Smlouvy (veřejné zakázky) a také po dobu trvání jiných závazků vyplývajících ze Smlouvy (veřejné zakázky).
5. Smlouva je sepsána v pěti vyhotoveních s platností originálu, z nichž Objednatel obdrží tři výtisky a Dodavatel dva.

V Brně dne .. 5.2.2019

[redacted]

GC System a.s.
[redacted], předseda představenstva

V Praze dne 7.2.2019

[redacted]

ČR - Český úřad zeměměřický a katastrální
Ing. Karel Štencel, místopředseda úřadu

V Praze dne 06.02.2019

[redacted]

Alef Nula, a.s.
[redacted], předseda představenstva

ALEF NULA, a.s.
Pernerova 691/42, 186 00 Praha 8
IČ: 61858579 DIČ: CZ61858579

Příloha č.1 – Podrobná specifikace předmětu smlouvy a servisní parametry

1. DC switching – Datacentrová síť

Síťová LAN infrastruktura datového centra bude tvořena z následujících zařízení:

- 4ks Datacentrový přepínač, každý uvnitř se čtveřicí Fabric modulů a dvěma line kartami.
- 2ks Přepínač pro Out-of-Band Management

Pro zabezpečení vysoké redundance uvnitř datového centra bude na každé lokalitě použita technologie vPC. vPC doména je tvořena dvojicí Nexusů, na kterých je možné nakonfigurovat tzv. multi-chassis vPC port-channel, který má z pohledu okolních zařízení stejnou charakteristiku jakoby se jednalo o jedno zařízení. Každé ze zařízení, které tvoří vPC doménu je aktivní jak z pohledu zpracovávání paketů (data plane), tak z pohledu řízení (control plane). Propoj mezi přepínači představuje 2x 100G a využívají se datové porty, které se konfigurují jako tzv. peer-link, teda komunikační kanál samotné vPC domény. V rámci možnosti se všechna zařízení budou připojovat k této páteřní infrastruktuře formou vPC port-channelu.

Zařízení zároveň poskytují pro koncové stanice defaultní gateway. Pro tyto účely je potřeba využít technologii FHRP (first hop redundancy protocol) např. protokol HSRP, který zabezpečí virtualizaci na úrovni L3. Oddělení jednotlivých produkčních síti je logicky zabezpečeno pomocí VRF (Virtual Routing & Forwarding).

Routing v infrastruktuře bude zachován ve formě staticky nakonfigurovaných záznamů.

Datacentrový přepínač Nexus 9504 p/n N9K-C9504-B3-E - minimální požadavky na funkcionalitu jednoho zařízení, celkem budou dodány 4 kusy (2 HA dvojice dle schématu)

Parametr číslo	**Požadovaná funkcionalita/vlastnost jednoho zřízení**	**Způsob splnění požadované funkcionality/vlastnosti**	**Nabídnul Dodavatel**
1	Výrobce zařízení	Uvedení výrobce	Cisco Systems
2	Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Účastník zadávacího řízení hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	Cisco Nexus 9500 N9K-C9504
3	Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-

			c78-729404.html
4	Formát zařízení	Modulární	Modulární
5	Redundantní AC napájecí zdroj	ANO	ANO
6	Redundantní řídící modul	ANO	ANO
7	Kapacita interní sběrnice na 1 slot přepínače	3,2 Tbps	3,2 Tbps,
8	Minimální počet slotů v šasi pro umístění ethernet komunikačních modulů	4	4
9	Minimální počet neblokovaných portů typu 1/10/25GE s volitelným fyzickým rozhraním	96	96
10	Minimální počet 10GBASE-SR SFP+ pro každý kus přepínače	24	106
11	Minimální počet 1000BASE-T SFP pro každý kus přepínače	45	180
12	Minimální počet 100GBASE-CR4 5m kabelů pro každý kus přepínače	1	4
13	Minimální počet 10GBASE aktivní optický kabel SFP+ 5m pro každý kus přepínače	7	26
14	Minimální počet neblokovaných portů 40/100GE s volitelným fyzickým rozhraním typu QSFP	8	8
15	Podpora break-out modu 4x10/4x25GE/2x50GE pro každý 100GE port	ANO	ANO
16	Podpora 40GE rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4	ANO	ANO
17	Podpora OS patching bez narušení provozu	ANO	ANO
18	VXLAN bridging	ANO	ANO
19	VXLAN gateway	ANO	ANO
20	VXLAN routing	ANO	ANO
21	VXLAN with MP-BGP EVPN control plane	ANO	ANO
22	IEEE 802.3ad	ANO	ANO
23	IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)	ANO	ANO
24	Minimální počet konfigurovatelných LAG rozhraní	500	500
25	Minimálně 32 linek jako součást LAG rozhraní	ANO	ANO
26	Minimální počet aktivních VLAN	3900	3900
27	Podpora instance spanning-tree protokolu per VLAN	ANO, min. 500	ANO, 500

28	IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	ANO
29	Detekce protilehlého zařízení (např. LLDP)	ANO	ANO
30	Minimální počet MAC záznamů	60000	60000
31	QoS classification – ACL, DSCP, CoS based	ANO	ANO
32	QoS marking - DSCP, CoS	ANO	ANO
33	QoS – Priority Based Flow Control (IEEE 802.1Qbb)	ANO	ANO
34	Approximate Fair Droping	ANO	ANO
35	Možnost zobrazit využití bufferů per port a per queue v reálném čase	ANO	ANO
36	GRE (Generic Routing Encapsulation)	ANO	ANO
37	Minimální počet host IPv4 routes	400000	400000
38	First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	ANO
39	OSPFv2	ANO	ANO
40	BGP	ANO	ANO
41	ECMP	ANO, min. 64 cest	ANO, 64 cest
42	IGMPv2, IGMPv3, MLDv2	ANO	ANO
43	IGMP snooping	ANO	ANO
44	IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6	ANO	ANO
45	Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	ANO
46	Min. počet VRF instancí	1000	1000
47	Podpora kontroly autenticity operačního systému switche, podpora kontroly integrity operačního systému switche při bootování kontrolou digitálního podpisu. Nutné pro ověření, že operační systém switche nikdo před či při bootování nebyl nemodifikován.	ANO	ANO
48	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

49	First Hop Redundancy Protokol pro IPv6	ANO	ANO
50	OSPFv3	ANO	ANO
51	MP BGP	ANO	ANO
52	VLAN ACL	ANO	ANO
53	Real time line rate telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem)	ANO	ANO
54	Integrovaná Flow table	ANO, min. 32000 záznamů	ANO, 32000 záznamů
55	Control Plane Policing	ANO	ANO
56	Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače	ANO	ANO
57	Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů	ANO	ANO
58	Podpora NETCONF/YANG	ANO	ANO
59	Streaming telemetrie - gRPC/GPB transport	ANO	ANO
60	Streaming telemetrie – time-based a event- based triggers	ANO	ANO
61	Python scripting	ANO	ANO
62	Puppet, Chef programming	ANO	ANO
63	Power-on autoprovisioning	ANO	ANO
64	CLI rozhraní	ANO	ANO
65	SSHv2	ANO	ANO
66	SNMPv3	ANO	ANO
67	NTPv3 server	ANO	ANO
68	RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	ANO
69	TACACS+ klient	ANO	ANO
70	Port mirroring (SPAN)	ANO	ANO
71	Vzdálený port mirroring (Encapsulated Remote SPAN) nebo ekvivalentní	ANO	ANO
72	Počet SPAN spojení	4	4

73	Syslog	ANO	ANO
74	Role Based Access Control	ANO	ANO
75	Podpora jumbo rámců	ANO	ANO
76	USB či sériová konzolová linka	ANO	ANO
77	Podpora SNMPv2c	ANO	ANO

Přepínač pro Out-of-Band management Catalyst 2960 p/n WS-C2960X-48TD-L – Minimální požadavky na funkcionalitu jednoho zařízení, celkem budou dodány 2kusy

OoB přepínače budou sloužit pro připojení management portů infrastrukturních zařízení za účelem vzdáleného přístupu na tyto zařízení.

Parametr číslo	**Požadovaná funkcionalita/vlastnost**	**Způsob splnění požadované funkcionality/vlastnosti**	**Nabídnul Dodavatel**
1	Výrobce zařízení	Uvedení výrobce	Cisco Systems
2	Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Účastník zadávacího řízení hlavní produktové číslo nabízeného zařízení)	Uvedení produktového čísla	Cisco Catalyst 2960-X WS-C2960X-48TD-L
3	Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	Uvedení požadovaného odkazu	https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
4	Třída zařízení - L2 switch	ANO	ANO
5	Velikost (výška) zařízení	max. 1RU	1RU
6	Počet 10/100/1000Mbit/s RJ45 Ethernet portů	min. 48	48
7	Počet 10Gbit/s SFP+ Ethernet portů	min. 2	2
8	Wirespeed (neblokující) na všech portech	ANO	ANO
9	Výkonnostní parametry		
10	Propustnost L2/L3 přepínacího systému	min. 104Gbit/s	104Gbit/s
11	Minimální paketový výkon přepínače	min. 130 milionů	130 milionů paketů/vteřinu

		paketů/vteřinu	
12	Vlastnosti stohování		
13	S okolními prvky tvoří virtuální přepínač - t.j. celek je jediná entita pro L2 i L3 protokoly	ANO	ANO
14	S okolními prvky tvoří virtuální přepínač - t.j. celek má jediný control plane	ANO	ANO
15	S okolními prvky tvoří virtuální přepínač - t.j. celek má jedinou konfiguraci	ANO	ANO
16	S okolními prvky tvoří virtuální přepínač - t.j. celek se kompletně spravuje, konfiguruje a troubleshootuje naráz, z jediného místa. Spravovat, konfigurovat a troubleshootovat každý prvek zvlášť, autonomně, se nepřipouští.	ANO	ANO
17	Počet přepínačů, které mohou vytvořit virtuální přepínač	min. 8	8
18	Virtuální přepínač podporuje distribuované přepínání paketů	ANO	ANO
19	Možnost předkonfigurace neexistujícího přepínače ve virtuální přepínači (před připojením fyzického přepínače)	ANO	ANO
20	Seskupení portů (IEEE 802.3ad) mezi různými prvky virtuálního přepínače	ANO	ANO
21	Kterýkoli prvek virtuálního přepínače může být jeho řídícím prvkem (1:N redundance)	ANO	ANO
22	IEEE 802.3-2005	ANO	ANO
23	Podpora "jumbo rámců" do velikosti 9k	ANO	ANO
24	IEEE 802.3ad (LACP)	ANO	ANO
25	Minimální počet LACP skupin 24	ANO	ANO
26	Minimální počet linek v jedné LACP skupině = 8	ANO	ANO
27	IEEE 802.1Q	ANO	ANO
28	Minimální počet aktivních VLAN 1000	ANO	ANO
29	Podpora IEEE 802.3az	ANO	ANO

30	HW připravený na nasazení IEEE 802.1ae	ANO	ANO
31	IEEE 802.1s - Multiple spanning tree	ANO	ANO
32	IEEE 802.1w - Rapid spanning Tree	ANO	ANO
33	IEEE 802.1p	ANO	ANO
34	Podpora STP instance per VLAN s 802.1Q tagováním BPDU (například PVST+), minimální počet podporovaných STP instancí = 64	ANO	ANO
35	LLDP a LLDP-MED	ANO	ANO
36	Podpora IPv4 a IPv6 statického směrování	ANO	ANO
37	Podpora IPv4 a IPv6 QoS	ANO	ANO
38	Hardware podpora IPv4 a IPv6 ACL	ANO	ANO
39	Podpora IGMP Snooping v1/v2/v3	ANO	ANO
40	Podpora MLD snooping v1/v2	ANO	ANO
41	DHCP snooping	ANO	ANO
42	IPv6 DHCP snooping	ANO	ANO
43	Podpora ověřování 802.1X - minimálně 1024 ověřených uživatelů na systém	ANO	ANO
44	Podpora ověřování MAC adres	ANO	ANO
45	Podpora zařazování do VLAN a přidělení přístupových filtrů na základě 802.1X ověření	ANO	ANO
46	Podpora zařazování do VLAN a přidělení přístupových filtrů na základě MAC-autentizace	ANO	ANO
47	Ověřování přístupu do sítě s podporou odlišných Guest VLAN (nedojde k pokusu o přihlášení), Fail VLAN (přihlášení selže) a Critical VLAN (nedostupnost RADIUS serveru)	ANO	ANO
48	Podpora kontroly autenticity operačního systému switche, podpora kontroly integrity operačního systému switche při bootování kontrolou digitálního podpisu. Nutné pro ověření, že operační systém switche nikdo před či při bootování nebyl nemodifikován.	ANO	ANO

49	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
50	Podpora IP source Guard pro IPv4	ANO	ANO
51	Podpora Source Address Validation pro IPv6 s využitim informaci obsažených v DHCPv6 a SLAAC	ANO	ANO
52	CLI rozhraní	ANO	ANO
53	SSHv2, Telnet	ANO	ANO
54	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	ANO
55	SNMPv2c	ANO	ANO
56	SNMPv3	ANO	ANO
57	Sériová nebo USB konzolová linka	ANO	ANO
58	AAA ověřování uživatelů (autentizace, autorizace, accounting) -RADIUS, TACACS+	ANO	ANO
59	Port mirroring	ANO	ANO
60	Traffic mirroring	ANO	ANO
61	Vzdálený mirroring (RSPAN)	ANO	ANO
62	Podpora více monitorujících portů současně	ANO	ANO

2. DWDM vrstva

DWDM vrstva - minimální požadavky na funkcionalitu jednoho zařízení NCS 2000 p/n NCS2K-TNCS-O-K9= Transport Node Controller celkem budou dodány 4ks (2 dvojice dle schématu)

Na základě požadavků Zadavatele nabízíme řešení postavené na platformě Cisco NCS 2000. NCS 2000 je přímí nástupce zařízení Cisco ONS 15454 a moduly používané v Cisco ONS 15454 je možné provozovat a používat v zařízení NCS 2000 (neboli při přechodu z jednoho do druhého se jedná o upgrade řešení).

V rámci nabízeného řešení předpokládáme využití komponent současného DWDM řešení, konkrétně modulů pro 4G FC během migrace na 8G FC a to během přechodu z původního řešení na nové řešení.

Nabízené řešení plně splňuje požadavky Zadavatele uvedené níže.

Více informací o zařízení lze najít na stránkách výrobce na odkazu níže:

https://www.cisco.com/c/en/us/products/collateral/optical-networking/network-convergence-system-2000-series/data_sheet_c78-729221.html

Parametr Číslo	**Požadovaná funkcionalita/vlastnost jednoho zařízení**	**Způsob splnění požadované funkcionality/vlastnosti**	**Nabídnul Dodavatel**
1	**Základní vlastnosti**		
2	Navržené DWDM zařízení je plně kompatibilní se stávající síťovou infrastrukturou postavenou na přepínačích Catalyst 6500 Cisco Systems a SAN přepínačích Cisco MDS. V případě migrace na technologii, která nevyužívá současných komponent, bude toto doloženo veřejným odkazem na stránkách výrobce například v sekci matice kompatibility.	ANO, buď se jedná o upgrade nebo je doloženo odkazem na veřejné stránky výrobce	ANO, jedná se o upgrade
3	Formát zařízení	aktivní DWDM systém, modulární s volnými sloty pro další rozšíření	ANO, modulární systém s 6 sloty celkem a volnými sloty pro rozšíření
4	Instalace systému do 19-ti palcového racku	ANO	ANO
5	Možnost více velikostí šasi pro různé nároky na prostor instalace a počet modulů v jednotlivých šasi	ANO	ANO, existuje možnost 2-slotového, 6-slootovoého, 15-slotového
6	Podpora AC i DC napájecích zdrojů	ANO	ANO

7	Redundantní napájení s podporou hot-swap	ANO, minimálně 1+1 redundance, 230 V AC pro zařízení dodaná do záložního centra, 48V DC pro zařízení dodaná do produkčního centra zdroj s napájecím kabelem v rámci dodávky Zařízení bude vybaveno maximálním počtem napájecích zdrojů, který je v šasi podporován Zařízení musí být schopno pracovat bez omezení i v případě výpadku poloviny napájecích zdrojů.	ANO
8	Redundantní ventilátory	ANO, Zařízení bude vybaveno maximálním počtem ventilátorů	ANO
9	Redundantní řídící procesory v šasi	ANO, zařízení bude vybaveno redundantním i řídícími procesory	ANO
10	DWDM systém podporuje zabudovanou funkcionalitu OTDR (Optical Time Domain Reflectometry) s přesností měření +/- 10 metrů při vzdálenosti lokalit 50km.	SPLŇUJE, zařízení bude vybaveno HW vybaveno funkcionalitou OTDR	ANO, zařízení je vybaveno řídícími kartami s OTDR funkcionalitou

11	Možnost použití minimálně 40 kanálů ve spektru (C-band, 100GHz spacing) bez nutnosti výměny HW v rámci dodávky s podporou 200Gbit/s na každém kanálu	ANO	ANO
12	Podpora optických kanálů min. 10G/40G/100G	ANO	ANO
13	Řešení DWDM přenosového systému musí být dostatečně flexibilní pro budoucí implementaci nových služeb, které v době zadání ještě nejsou známy. Mezi takové služby může patřit např. implementace přímých logických propojů na bázi různých technologií.	ANO, podporovány minimálně následující klientské signály GE/10GE/40 GE/1 00GE, 1/2/4/8/10/16 G FC, STM-1/4/16/64/256 , OTU-1/2/2e/4 v době podávání nabídky	ANO, uvedené služby jsou podporovány v době podání nabídky
14	Podpora topologií bod-bod, kruh, mesh	ANO	ANO
15	Podpora ROADM (Reconfigurable Optical Add/Drop Multiplexor) – Optionally	ANO	ANO
16	Každý uzel DWDM sítě v rámci dodávky bude realizován na bázi rekonfigurovatelných optických add-drop multiplexorů (ROADM), s možností vzdálené rekonfigurace procházejících i vybočujících kanálů.	ANO	ANO
17	Ekvalizace spektra pomocí VOA (Variable Optical Attenuator) pro všechny průchozí i odbočované kanály	ANO	ANO
18	Elektronicky laditelné útlumové články (VOA) budou umožňovat vyrovnání optických signálů před vstupem do optického zesilovače a jejich vyladění jednotlivých linkových signálů.	ANO	ANO

19	Kompenzace chromatické disperze pro všechny požadované kanály spektra, pokud bude v daném řešení nutné	ANO	ANO
20	Monitorování na optické vrstvě, OTN a payload úrovni	ANO	ANO
21	Automatické bezpečnostní vypínání laseru dle specifikace ITU-T G.664	ANO	ANO
22	Automatické vypínání laseru na klientském rozhraní při výpadku páteřního spoje	ANO	ANO
23	Možnost sledování/nastavování optického výkonu individuálně pro každý kanál	ANO	ANO
24	Automatické řízení zisku optického zesilovače umožňující reakcí na rychlé změny (výpadky) i pomalé změny (stárnutí optického vlákna)	ANO	ANO
25	Všechny trunkové porty vysílající na DWDM vlnové délce musí být plně laditelné přes všech 40 optických kanálů.	ANO	ANO
26	Řešení DWDM musí být spravovatelné jednotným end-to-end provisioning, performance a fault management nástrojem.	ANO	ANO
27	Integrovaná GUI aplikace pro správu jednotlivých šasi a uzlů – topologie sítě, pohled na uzel/šasi/modul, alarmy, statistiky, funkční schémata uzlů, Správa celého uzlu sesazeného z více šasi jako jeden celek	ANO	ANO
28	Využité zesilovače musí podporovat automatické řízení zisku s reakcí na rychlé i pomalé změny.	ANO	ANO
29	Z hlediska provisioningu musí řešení umožnit sestavení optického kanálu mezi koncovými uzly pouze za použití vzdálené konfigurace mezilehlých uzlů.	ANO	ANO
30	V případě, že v rámci např. větších lokalit bude využito více chassis na lokalitu, musí management nástroj spravovat takovýto set zařízení jako jeden logický celek.	ANO	ANO

31	Klientské signály se připojují k servisním kartám typu transponder/muxponder/xponder, které jsou vybaveny vyměnitelnými optickými moduly (transceiver).	ANO	ANO
32	DWDM přenosový systém je možné rozšířit o modul zajišťující šifrování přenášeného provozu při minimálně následující klientské signály – 10GE LAN PHY. Šifrovací modul musí být k dispozici při podávání nabídky a je požadováno poskytnutí produktového značení a produktového listu (datasheet).	ANO	ANO, 15454-M-WSE-K9= https://www.cisco.com/c/en/us/products/collateral/optical-networking/ons-15454-series-multiservice-transport-platforms/datasheet-c78-729795.html
33	Podpora optických DWDM signálů připojených z externích zařízení podle ITU-T G.698.2 (Alien Wavelength)	ANO	ANO
34	Podpora transponderů s podporou FEC (G.975) i EFEC (G.975.1) a zabezpečení přenášeného provozu formou šifrování minimálně AES-256 s podporou klientských rozhraní 10 GE, OTU2, OTU2e, 8G FC.	ANO	ANO
35	Podpora servisních karet typu xponder s podporou FEC na trunkových portech a s podporou klientských rozhraní 10GE, 16G FC, 100GE.	ANO	ANO
36	GUI aplikace pro kompletní návrh systému – zadání topologie, parametrů vláken, požadavků na klientské rozhraní a propojení koncových uzlů včetně možnosti návrhu s přípravou na plánované propojení uzlů v budoucnu. Výstupem návrhu jsou použité vlnové délky, analýza optických cest a jejich parametrů - útlum, OSNR, CD, PMD, nastavení zesilovačů.	ANO	ANO
37	Řídící OSC kanál přenášený spolu se spektrem uživatelských kanálů na vlnové délce 1510 nm s možností datového uživatelského kanálu s ethernetovým rozhraním	ANO	ANO

38	Všechny DWDM uzly v dohledovém systému budou přístupné s použitím optického dohledového kanálu (OSC).	ANO	ANO
39	Všechny DWDM uzly složené z 2 a více chassis musí být dohlížené jako jeden síťový prvek.	ANO	ANO
40	Měření útlumu vlákna mezi sousedními uzly – hodnota je zobrazená v rámci managementu	ANO	ANO
41	Dohledový systém bude podporovat mechanismus pro monitorování úrovně optického signálu pro každou vlnovou délku a bude schopen naladit je v případě přidání nové vlnové délky nebo změny charakteristiky optického vlákna v průběhu času.	ANO	ANO
42	Podpora SNMP v1/2c/3	ANO	ANO
43	Podpora IPv4 a IPv6 pro management přístup	ANO	ANO
44	Možnost ověřování přistupování uživatelů do grafického rozhraní pro management minimálně pomocí RADIUS	ANO	ANO
45	Bezvýpadkový upgrade programového vybavení	ANO	ANO
46	Požadavky na konfiguraci systému	ANO	ANO
47	Řešení postavené jako dvě nezávislé topologie point to point mezi dvěma lokalitami, celkem minimálně 4 uzly, 2 uzly v každé lokalitě	ANO	ANO
48	Řešení je navržené dle parametrů optických vláken uvedených v odstavci výše.	ANO	ANO
49	Pro všechny MPO/MTP konektory směrem ke klientským zařízením (LAN/SAN switch) bude součástí řešení rozpletení MPO konektorů na LC konektory tak, aby směrem ke klientským transceiverům bylo možné využívat pouze LC/LC optické patchcordy.	ANO	ANO

50	Přenos 2x 10GE LAN PHY v rámci jedné topologie (celkem 4x 10GE LAN PHY v celém řešení) jako optických DWDM signálů připojených z externích zařízení podle ITU-T G.698.2 (Alien Wavelength). Součástí řešení musí být optické transceivery na DWDM vlnových délkách instalovatelných a kompatibilních s okloní infrastrukturou tak, aby v každé fázi implemetace bylo funkční celé řešení .	ANO	ANO
51	Přenos 4x 8G FC v rámci jedné topologie (celkem 8x 8G FC v celém řešení). DWDM systém musí provádět OEO (Optical - Electrical - Optical) regeneraci příchozího 8G FC signálu na servisní kartě typu muxponder/transponder/xponder. Do DWDM systému bude připojen 8G FC na vlnové délce 850 nm pomocí multimodového vlákna.	ANO	ANO
52	Navržené řešení je v rámci dodávky vybaveno v každém DWDM uzlu servisními kartami typu muxponder/transponder/xponder s volnými kapacitami pro budoucí rozšíření o 1x 10 GE nebo 1x 8G FC a to pouze přidáním transceiverů případně povýšením licence.	ANO	ANO
53	Součástí dodaného řešení bude redundantní systém pro správu DWDM přenosového systému. Za redundantní řešení je považováno: Management systém umožňující z klientských stanic přímé připojení na GUI DWDM zařízení v případě, kdy je možné spravovat z této klientské stanice všechna zařízení v DWDM síti současně a provádět veškerá nastavení v DWDM systému. Požadováno je připojení minimálně z 5 klientských stanic současně. V případě této varianty je požadována dodávka licencí pro minimálně 5 klientských stanic. Management systém využívající centrální aplikaci běžící na serverech v datovém centru umožňující spravovat všechna zařízení v DWDM síti současně a provádět veškerá nastavení v DWDM systému. V případě této varianty je požadována dodávka redundantního řešení využívající 2	ANO	ANO, Využívá se management systém umožňující správu z klientských stanic přímo na GUI DWDM zařízení

	virtuálních serverů pod VMWare, dodávky licencí za management SW a 5 klientských stanic a licencí operačního systému.		
54	Klientská část management SW běžící na klientských stanicích podporuje minimálně operační systémy Windows 7, Windows 10, Windows server 2008 nebo novější.	ANO	ANO

3. Load Balancing vrstva

Na základě uvedených parametrů nabízíme řešení postavené na platformě F5. Jedná se o 4 kusy hardwarového zařízení Big-IP i5800 s LTM a ASM modulem (p/n F5-BIG-LTM-I5800) .

Parametr Číslo	**Požadovaná funkcionalita/vlastnost**	**Způsob splnění požadované funkcionality/vlastnosti**	**Nabídnul Dodavatel**
1	Velikost hw řešení - 1RU	ANO	ANO
2	Podpora rozhraní až 24x 10GE (SFP+)	ANO	ANO
3	Podpora rozhraní až 4x 40GE (QSFP+)	ANO	ANO
4	L4 propustnost minimálně 60 Gbps full- duplex	ANO	ANO
5	Podpora minimálně 12 000 000 L4 spojení za sekundu	ANO	ANO
6	Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů až do 7. vrstvy OSI (ftp, dns, https/http, sip, …)	ANO	ANO
7	Klient/Server NAT/PAT	ANO	ANO
8	Podpora různých typů load-balancingu, minimálně všechny dále uvedené: Kruhová metoda s vážením Podle počtu navázaných spojení Podle otisku zdrojové a cílové adresy Podle URL a cookie Na základě SNMP (např. zátěže procesorů) Podle vah pro skupiny Na základě velikosti odezev od serverů	ANO	ANO
9	Podpora zajištění konektivity uživatelů ke konkrétnímu serveru (persistence) na základě IP adresy, L4 payloadu, HTTP cookie (včetně vkládané loadbalancerem), HTTP obsahu, HTTP hlavičky, RADIUS atributů, RTSP hlavičky, SIP hlavičky, SSL Session ID	ANO	ANO

10	Podpora různých typů health monitoringu - ICMP, DNS, HTTP, TCP/UDP port, SSL Hello, SMTP, RADIUS, LDAP, WMI…	ANO	ANO
11	Možnost kombinace více metod monitoringu (AND/OR)	ANO	ANO
12	Podpora modifikace provozu: Vložení/přepsání cookie Modifikace URL Možnost vložit zdrojovou IP do L7 hlavičky Modifikace HTTP obsahu	ANO	ANO
13	Podpora šablon pro konfiguraci balancingu aplikací – např. Microsoft Exchange Server 2010 a 2013 Client Access Servers,Citrix XenApp a XenDesktop	ANO	ANO
14	Možnost tyto šablony upravovat dle potřeb zákazníka	ANO	ANO
15	Podpora TCP multiplexingu	ANO	ANO
16	Podpora multipath TCP (MPTCP)	ANO	ANO
17	Podpora symetrické akcelerace Citrix ICA	ANO	ANO
18	Podpora ICAP	ANO	ANO
19	Podpora komprese	ANO	ANO
20	Podpora cachování	ANO	ANO
21	Podpora filtrování paketů	ANO	ANO
22	Podpora QoS – markování, rate-limiting	ANO	ANO
23	Podpora TCP SYN cookie	ANO	ANO
24	Podpora SDN služeb – VXLAN virtualizace sítě dokoupením licence	ANO	ANO
25	Podpora NVGRE a Transparent Ethernet Bridging tunelu dokoupením licence	ANO	ANO
26	TDS/ MSSQL DB Proxy	ANO	ANO
27	Podpora Financial Information eXchange (FIX) protokolu	ANO	ANO
28	Možnost přidávat zákaznické požadavky na základě skriptování	ANO	ANO
29	SSL akcelerace	ANO	ANO

30	Podpora SSL certifikátů podepsaných SHA-2 metodou	ANO	ANO
31	Podpora TLS 1.2	ANO	ANO
32	Podpora AES-GCM a ECC pro TLS 1.2	ANO	ANO
33	Podpora STARTTLS pro SMTP provoz	ANO	ANO
34	Podpora šifrování pomocí Suite B, ECDSA, AES-GCM a SafeNet Network HSM	ANO	ANO
35	Možnost pracovat až s 4096-bitovými klíči	ANO	ANO
36	Podpora IPv4/IPv6 brány	ANO	ANO
37	Plná podpora IPv6	ANO	ANO
38	Možnost přidání Web Aplikačního Firewalu a ICSA certifikovaného Network Firewalu jen pomocí rozšíření SW	ANO	ANO
39	Podpora 802.1Q	ANO	ANO
40	Podpora Video Quality of Experience (QoE)	ANO	ANO
41	Podpora sFlow	ANO	ANO
42	Podpora IPFIX	ANO	ANO
43	Správa přes GUI, CLI	ANO	ANO
44	Podpora SNMP (1, 2c a 3)	ANO	ANO
45	Podpora SSH	ANO	ANO
46	Podpora syslogů per aplikace	ANO	ANO
47	Podpora režimu redundance se synchronizací stavových tabulek	ANO	ANO
48	Podpora redundantních clusterů Active- Standby i Active-Active	ANO	ANO
49	Možnost zapojit do redundantniho clusteru různé typy HW	ANO	ANO
50	Dostupnost jak hardwarového tak i virtuálního řešení	ANO	ANO
51	Podpora otevřeného API pro nástroje třetích stran	ANO	ANO
52	Podpora virtualizace – jak kontexty, tak i separace adresního prostoru (aka VRF, route domain)	ANO	ANO

53	Možnost vytvořit minimálně 4 kontexty (VDC, vCMP)	ANO	ANO
54	Nezávislé rozhraní pro management	ANO	ANO
55	Vestavěná ochrana proti DoS útokům	ANO	ANO
56	Integrace s nástrojem na detekci zranitelností webových aplikací	ANO	ANO
57	Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	ANO	ANO
58	Možnost doprogramovat si filtrovaci pravidla pro aplikace	ANO	ANO
59	Ochrana AJAX a JSON aplikací	ANO	ANO
60	Ochrana proti OWASP Top 10 útokům	ANO	ANO
61	Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	ANO	ANO
62	Podpora Captcha metody – automatické odlišení skutečných uživatelů od robotů	ANO	ANO
63	Integrovaný XML firewall	ANO	ANO
64	Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…	ANO	ANO
65	Automatické nahrávání a aplikování nových signatur	ANO	ANO
66	Podpora pozitivního a negativního bezpečnostního modelu	ANO	ANO
67	Blokování útočníků na základě geolokace	ANO	ANO
68	Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP	ANO	ANO
69	Ochrana SMTP a FTP na alikační úrovni	ANO	ANO
70	Podpora SSL (šifrování a dešifrování)	ANO	ANO
71	Podpora ECDSA a podpora hybridních certifikátů (DSA/ECDSA/RSA)	ANO	ANO
72	Podpora symetrického šifrování včetně šifer Camellia	ANO	ANO
73	Podpora HTTP Strict Transport Security (HSTS)	ANO	ANO
74	Podpora HTTP/2	ANO	ANO

75	Podpora akcelerace - Konsolidace TCP spojení od klienta směrem k serveru tj. Z několika spojení od uživatele udělat jedno spojení na server - Caching - Komprese - Možnost optimalizace TCP stacku zvlášť směrem k uživateli a směrem k severu	ANO	ANO
76	Podpora různých typů reportů – PCI, geolokační reporty	ANO	ANO
77	Podpora standardů PCI DSS, HIPAA, Basel II a SOX	ANO	ANO
78	Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint	ANO	ANO
79	Podpora application visibility a reportingu – monitorování URI	ANO	ANO
80	Možnost importu zranitelnosti aplikací z alespoň 2 následujících skenerů: • Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning	ANO	ANO
81	Podpora REST API	ANO	ANO
82	Autentizace klientů přes LDAP/Radius	ANO	ANO
83	Podpora application visibility a reportingu – monitorování URI	ANO	ANO
84	Podpora aplikačního firewallu ve virtuálních kontextech	ANO	ANO
85	Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	ANO	ANO
86	Možnost aktivovat L4-7 LoadBalancing, ICSA certifikovaný webový a síťový firewall, SSL VPN na jedné platformě HW	ANO	ANO
87	Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	ANO	ANO

88	Možnost přidat vlastní funkce pomocí skriptování	ANO	ANO
89	Podpora Active-Active, Active-Passive módů	ANO	ANO
90	Granulární logování / logování per aplikace	ANO	ANO
91	Podpora vysokorychlostního logování (high-speed logging)	ANO	ANO
92	K dispozici jako autonomní box nebo ve formě šasi	ANO	ANO
93	Management: sériový port, GUI, příkazový řádek, iLO	ANO	ANO
94	Podpora login a logout stránek pomocí AJAX/JSON	ANO	ANO
95	Mitigace DDoS útoků založená na behaviorální analýze	ANO	ANO
96	Povoleni jednotlivych HTTP metod pro jednotliva URL	ANO	ANO
97	Podpora více logovacích profilů	ANO	ANO
98	Podpora WebSocketu	ANO	ANO
99	Automatické přidávání IP adres útočících na sedmé vrstvě na blacklist	ANO	ANO
100	Prevence „Session Hijacking“	ANO	ANO
101	Detekce anomálií sledováním ID koncové stanice uživatele	ANO	ANO
102	Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům)	ANO	ANO
103	Podpora jumbo rámců	ANO	ANO
104	USB či sériová konzolová linka	ANO	ANO

4. Vrstva Firewallů (NGFW)

NGFW vrstva - minimální požadavky na funkcionalitu jednoho kusu zařízení Cisco Firepower 4120 Threat Defense (p/n FPR4120-FTD-HA-BUN), celkem *budou dodány 4ks (2 HA dvojice dle schématu)*

Next Generation Firewall – Cisco Firepower

V dnešní době již není možné se spolehnout na tradiční přístup filtrování provozu pouze na základě IP adres a komunikačních portů. Většina útoků probíhá po standardních portech jako je http komunikace, případně je zašifrována a posílána přes protokol HTTPS. Pro obranu sítě je proto nutné využít zařízení typu Next Generation Firewall, které dokáže provoz analyzovat až do úrovně komunikující aplikace a zastavit hrozby, které mohou v síti procházet.

Aktuální trendy v oblasti útoků vyžadují sofistikovanější metody inspekcí hrozeb, jejich detekci, blokaci a případnou automatizovanou remediaci. Cisco nabízí následující varianty řešení:

- ASA firewally s NextGen funkcionalitami v podobě Firepower Services
  - Jde o tradiční Cisco ASA firewall, který je rozšířen o možnosti „Next Generation"
- Firepower NextGen (FTD)
  - FTD vznikl jako unifikovaný systém Next Generation Firewallu, který slučuje vlastnosti Cisco ASA firewallu a Firepower (Sourcefire) aplikační inspekce. FTD nabízí L4 Firewall s VPN spojený s pokročilou aplikační SNORT ochranu (AVC, IPS, reputace, AMP, SSL dešifrování, ..)

Mezi klíčové vlastnosti Cisco Firepower patří:

- IPS nebo IDS detekční a ochranný systém se schopností automatického ladění souboru IPS/IDS signatur podle sledování prostředí a automatickým vyhodnocením stupně nebezpečnostní útoků v relevanci s metodou útoku a zranitelností cílového systému
- Automatické potlačení útoku (Remediation) na základě korelace událostí s nastavenými pravidly pro odpovídající typy reakce (např. signalizace požadavku směrem do jiných síťových zařízení pro odpojení stanice, nastavení přístupového filtru, přesměrování, apod.)
- Interní korelace událostí (typ útoku, komunikace v botnet síti, přenos malware, apod.) pro automatickou detekci kompromitovaných stanic
- Kontinuální analýza síťového prostředí s automatickou reakcí na porušení pravidel (compliancy) – např. detekce nepovoleného OS v určitém segmentu sítě, vybočení ze „standardního" obrazu komunikace, apod.
- Detekce přenosu malware, včetně zero-day typů souborů, s možností retrospektivního monitorování (trajektorie přenosu souborů sítí: první stanice která soubor získala, protokoly a metody přenosu v rámci sítě, reakce senzorů nebo agentů na koncových stanicích na daný malware, apod.)
- Aplikační firewall s možností definice vlastních aplikací (podpora OpenAppID aplikačních signatur)
- URL filtrace podle web kategorií, reputace, konkrétních URL
- Integrace Security Intelligence blacklistů – DNS, URL, známé adresy botnet sítě, problematické stroje v Internet
- Antimalware ochrana – analýza přenášených souborů s možností dynamické analýzy a sandboxing se záznamem přenosu všech souborů sítí pro následnou retrospektivní analýzu

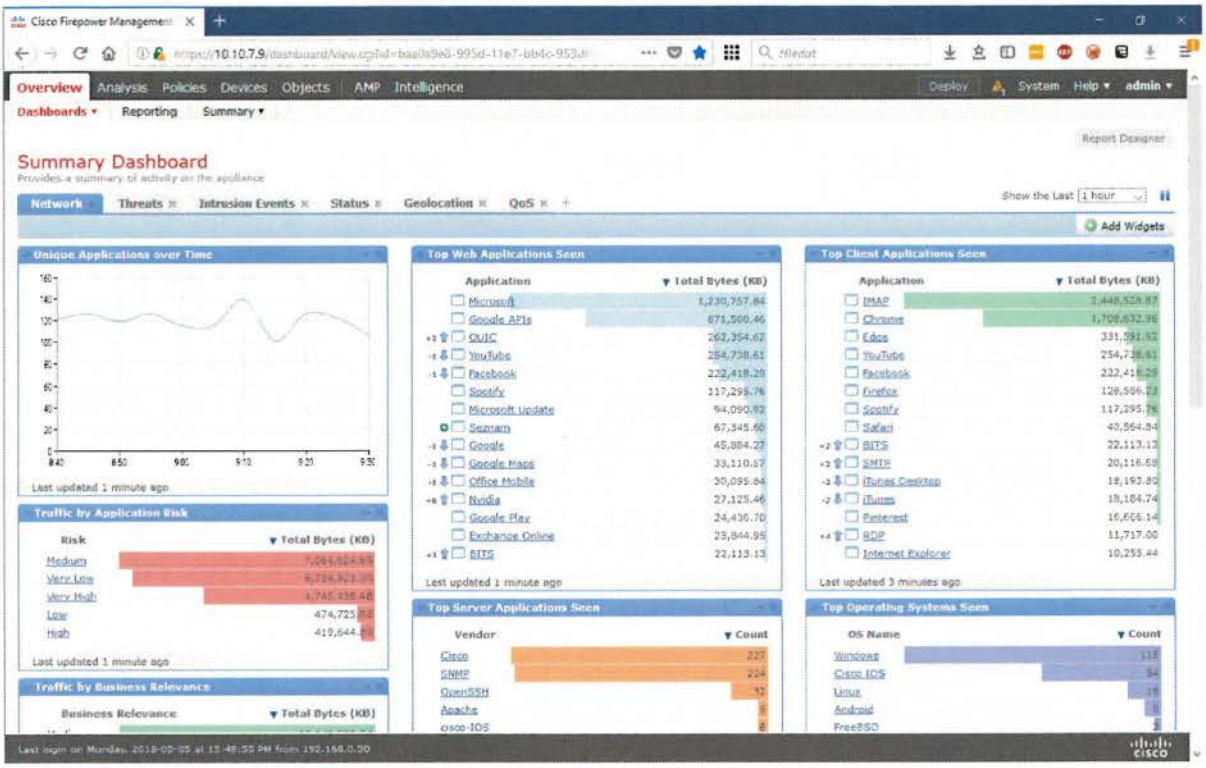
Cisco Firepower a Management

Cisco Firepower nextGen řešení je možné spravovat pomocí centrálního managementu FMC (Firepower Management Center)

FMC platforma je schopna dlouhodoběji zaznamenávat bezpečnostní události, provádět nad nimi a dalšími analýzu (např. detekovaný operační systém, typ platformy, vzorek síťového chování, apod.) korelovat, automaticky vyhodnotit to co je v dané chvíli a v daném prostředí důležité, poskytovat ***retrospektivní informace o bezpečnostních incidentech*** i zpětně v čase a ***flexibilně generovat odpovídající reporty***.

Díky integraci a správě firepower NextGen FTD či Firepower services je pomocí FMC dále možné:

- vidět co se děje v síti nejen na úrovni IP adres, ale v širším kontextu,
- segmentovat a specificky aplikovat bezpečnostní pravidla na různé typy komunikace,
- nastavit přehledné, znovupoužitelné konfigurace bezpečnostních politik,
- zohlednit prostředí, ve kterém jsou systémy nasazeny,
- automaticky nastavit a vybrat IPS pravidla, která jsou v daném prostředí relevantní,
- filtrovat důležité incidenty před těmi méně důležitými na základě korelace skutečných zranitelností v síti a typech útoků,
- generovat události a akce na základě korelace více bezpečnostních incidentů, chování sítě, apod.
- automaticky a rychle reagovat na bezpečnostní incidenty,
- sledovat „compliancy" stanic v síti – tj. např. výskyt určitých typů OS v určitých částech sítě, způsob komunikace, apod.
- automaticky korelovat události na koncových stanicích a detekovat kompromitované,
- automaticky izolovat kompromitované stanice, pokud to vyžaduje firemní bezpečnostní politika,
- analyzovat soubory přenášené sítí na skryté hrozby - nedetekované tradičními AV
- spolupracovat se systémy řízení přístupu do sítě, SIEM, vulnerability managementem
- integrovat se s dalšími bezpečnostními systémy v síti, např. Identity Services Engine (ISE) přes rozhraní pxGrid pro získání doplňujících informací pro aplikaci bezpečnostních pravidel nebo aktivaci obranných opatření v síti.



Ve spolupráci s naší společností vám pomůžeme:

- Vybrat správné řešení, které bude splňovat požadavky na funkce a propustnost
- Navrhnout správný design zapojení a kooperace se stávajícími prvky ve vaší síti
- Proof of Concept
- Nastavení zařízení dle Vašich požadavků a našich znalostí
- Kontinuální sledování a vyhodnocování incidentů díky našemu CSirt týmu
- Analýza provozu a optimalizace nastavení, přizpůsobená typu provozu ve Vaší síti
- Pomoct při řešení konfiguračních nebo síťových problémů.

Parametr číslo	Požadovaná funkcionalita/vlastnost jednoho kusu zařízení	Způsob splnění požadované funkcionality/vlastnosti	Nabídnul Dodavatel
1	**Výkon a funkcionalita firewallu**		
2	Formát zařízení	Appliance, 1RU	1RU
3	Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	1
4	Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	8	8
5	Možnost rozšíření o moduly rozhraní	2	2
6	Možnost rozšíření o další 10Gb SFP+ rozhraní	8	8
7	Možnost rozšíření o další 40Gb SFP+ rozhraní	4	4

8	Redundantní zdroje	ANO	ANO
9	Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.15M/4.5M	15M/15M
10	Rychlost vytváření nových spojení přes stavový FW	Min. 250K/s	250K/s
11	Propustnost stavového firewallu (multiprotokolový režim)	Min. 30 Gbps	30 Gbps
12	Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 20 Gbps	20 Gbps
13	Propustnost aplikačního FW + IPS (next- gen FW, IPS) - (top parametry)	Min. 15 Gbps	15 Gbps
14	Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 8 Gbps	8 Gbps
15	Propustnost aplikačního FW + IPS (next- gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 5 Gbps	5 Gbps
16	VPN propustnost	Min. 10 Gbps	10 Gbps
17	Současný počet VPN spojení (IPSec/SSL)	Min. 15.000	15.000
18	Možnost min. 3 virtuálních kontextů pro FW	ANO	ANO
19	Podpora L3 (routovaného) módu s podporou NAT a PAT	ANO	ANO
20	Podporovaný počet VLAN	Min. 1024	1024
21	Podpora stateful failover	active/standby	active/standby
22	Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	ANO	ANO
23	Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	ANO	ANO
24	Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	ANO	ANO
25	Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	ANO	ANO
26	Dynamické směrování - podpora alespoň RIP, OSPF, BGP	ANO	ANO
27	Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	ANO	ANO
28	Podpora Policy based Routing	ANO	ANO
29	Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	ANO	ANO
30	Podpora filtrace IPv4, IPv6	ANO	ANO
31	Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	ANO	ANO
32	Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	ANO	ANO

33	Podpora inspekce IPv6 provozu	ANO	ANO
34	Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	ANO	ANO
35	Podpora NAT64 a DNS64	ANO	ANO
36	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
37	Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	ANO	ANO
38	Možnost rozšíření o funkce NextGen FW	ANO	ANO
39	Možnost rozšíření o funkce NextGen IPS	ANO	ANO
40	Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	ANO	ANO
41	Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	ANO	ANO
42	API rozhraní pro sdílení kontextových informací s dalšími systémy	ANO	ANO
43	Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	ANO	ANO
44	Podpora kontroly autenticity operačního systému zařízení, podpora kontroly integrity operačního systému zařízení při bootování kontrolou digitálního podpisu. Nutné pro ověření, že operační systém zařízení nikdo před či při bootování nikdo nemodifikoval.	ANO	ANO
45	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
46	Funkce IPS a anti-malware		
47	Možnost definovat typ provozu předávaný k inspekci do IPS	ANO	ANO
48	Podpora také IDS režimu – pasivního monitorování (TAP režim)	ANO	ANO
49	Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	ANO	ANO
50	Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	ANO	ANO
51	Podpora 802.1Q tagovaných rámců	ANO	ANO
52	Podpora různých IPS politik pro různé typy provozu	ANO	ANO
53	Inspekce pro IPv4 i IPv6	ANO	ANO
54	Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který	ANO	ANO

	může způsobit zahlcení systému		
55	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
56	Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	ANO	ANO
57	Podpora aplikace pro psaní zákaznických filtrů	ANO	ANO
58	Podpora importu komunitních filtrů/signatur Snort	ANO	ANO
59	IPS musí umět detekovat a blokovat útoky průzkumných aktivit	ANO	ANO
60	IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	ANO	ANO
61	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
62	IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře Zadavatele, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	ANO	ANO
63	Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	ANO	ANO
64	Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	ANO	ANO
65	Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	ANO	ANO
66	Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	ANO	ANO
67	Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	ANO	ANO
68	Možnost definice uživatelské vrstvy politik	ANO	ANO
69	Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	ANO	ANO
70	Různé politiky lze sdílet a aplikovat na různé senzory	ANO	ANO
71	Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na	ANO	ANO

	aktuálních databázích AV dodavatelů		
72	Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	ANO	ANO
73	Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	ANO	ANO
74	Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	ANO	ANO
75	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
76	Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, – pokud je později SW kód rozpoznán v operačním centru doddavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	ANO	ANO
77	Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	ANO	ANO
78	IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	ANO	ANO
79	Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	ANO	ANO
80	Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.	ANO	ANO
81	Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	ANO	ANO
82	Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	ANO	ANO
83	Podpora databází reputací adres v Internetu (Security Intelligence)	ANO	ANO
84	Funkce Next-Gen FW		
85	Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	ANO	ANO
86	Podpora pasivního monitorování (TAP režim)	ANO	ANO
87	Podpora 802.1Q tagovaných rámců	ANO	ANO
88	Podporovaných aplikací	Min. 3000	3500
89	Kategorie aplikací (nebezpečné, důležité, apod.)	ANO	ANO

90	URL kategorií	Min. 80	80
91	Katalogizovaných světových URL	Min. 280 milionů	290 milionů
92	Řízení přístupu k WWW - Web Usage Control (WCU)	ANO	ANO
93	Filtrace podle typů aplikací webových i ne-webových	ANO	ANO
94	Filtrace podle reputace serverů	ANO	ANO
95	SSL inspekce (dekrypce/enkrypce)	ANO	ANO
96	Security Inteligence database – známé uzly botnet sítí C&C	ANO	ANO
97	Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	ANO	ANO
98	Security Inteligence database – známé nebezpečné URL adresy a jmenné domény	ANO	ANO
99	Možnost integrovat vlastní reputační databáze	ANO	ANO
100	Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	ANO	ANO
101	Filtry mohou zohlednit roli a identitu uživatele	ANO	ANO
102	Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	ANO	ANO
103	Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	ANO	ANO
104	Rešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazeních:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti	ANO, vše požadované
105	Přehled o síťových spojení má poskytovat minimálně tyto informace:	Cas 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	ANO, vše požadované

		„Business impact“ aplikace Množství přenesených dat	
106	Správa		
107	Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	ANO	ANO
108	Přístup ke GUI http/https protokolem	ANO	ANO
109	Možnost vzdáleného přístupem protokolem ssh přímo do FW	ANO	ANO
110	Možnost přístupu k textovým logům (syslog) přímo ve FW	ANO	ANO
111	Možnost centrální správy při nasazení více firewallů	ANO	ANO
112	Při centrální správě: možnost sdílených bezpečnostních politik	ANO	ANO
113	Při použití clusteru se spravuje pouze jeden logický prvek	ANO	ANO
114	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
115	Zobrazení logů a událostí v grafickém rozhraní správy	ANO	ANO
116	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
117	Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	ANO	ANO
118	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
119	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
120	Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	ANO	ANO
121	Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	ANO	ANO

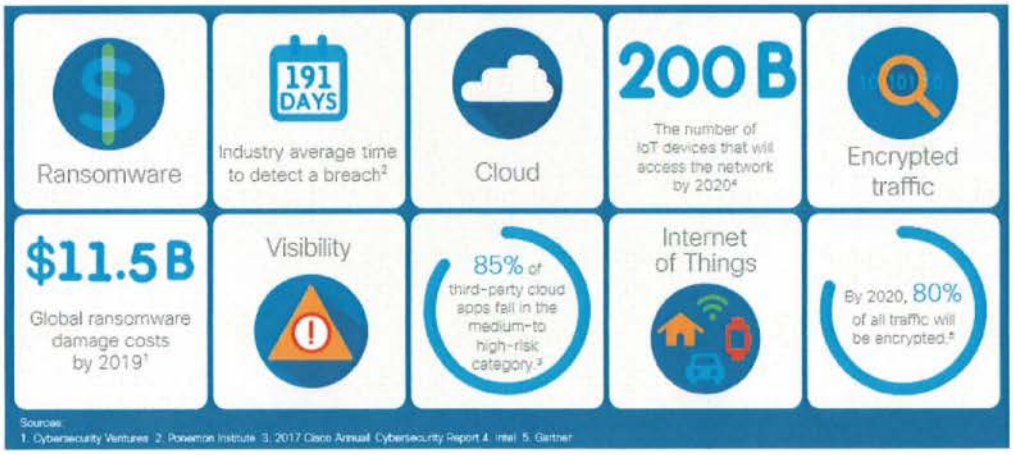
122	Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	ANO	ANO
123	Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	ANO	ANO
124	Pro reporty lze definovat template definující formát a obsah reportu	ANO	ANO
125	Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	ANO	ANO
126	V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top- N	ANO	ANO
127	Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	ANO	ANO
128	Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	ANO	ANO
129	Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	ANO	ANO
130	Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	ANO	ANO
131	Podpora posílání událostí formou syslog, email, SNMP na externí platformy	ANO	ANO
132	Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk	ANO, vše požadované
133	Podpora jumbo rámců	ANO	ANO
134	USB či sériová konzolová linka	ANO	ANO

5. Monitoring NetFlow

Monitoring NetFlow - minimální požadavky na funkcionalitu Cisco Stealthwatch Flow Rate Bundle (p/n ST-FR-BUN). Cisco ISE Virtual Machine Small (p/n R-ISE-VMS-K9=)

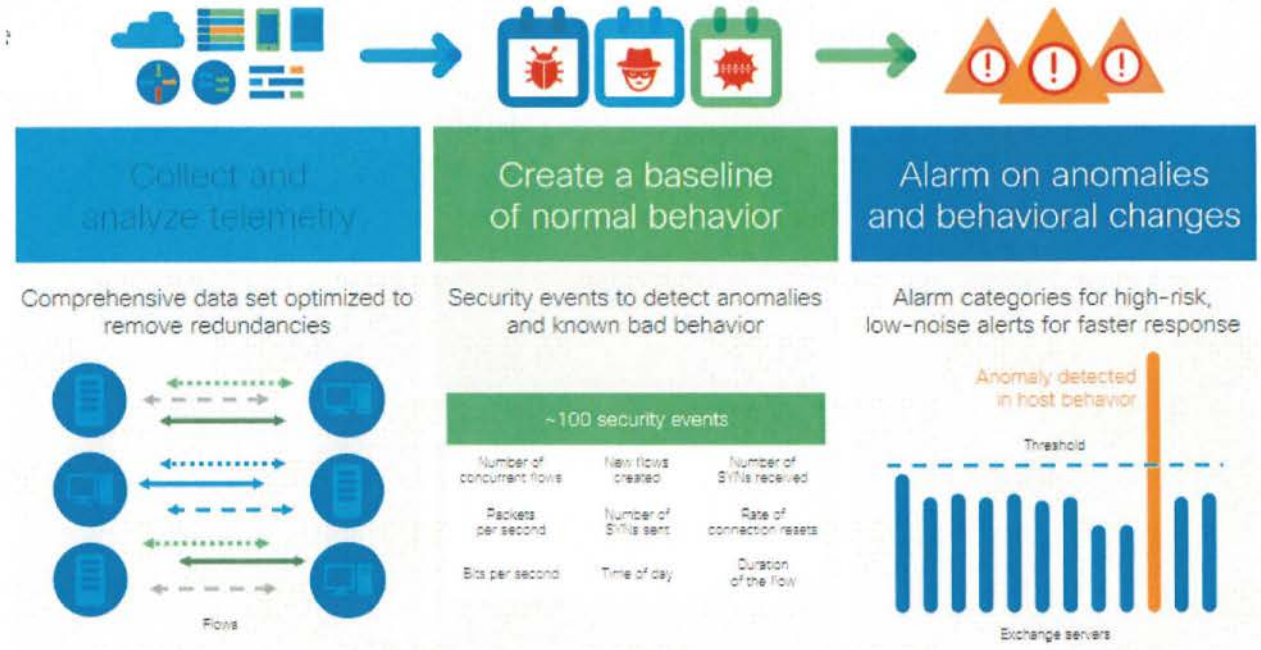
StealthWatch: neustálým zvyšováním komplexnosti enterprise sítí se vytvořilo mnoho slepých míst. V dnešní době se mnoho zaměstnanců připojuje z mnoha míst. Roste počet chytrých zařízení v síti i využívání veřejných cloudových služeb. K tomu se zvyšuje využívání šifrování provozu k zabezpečení soukromí a ochraně dat.

Všechny tyto aspekty využívají tvůrci škodlivých kódů k ukrytí a zamaskování své aktivity, aby zůstali neodhaleni a mohli tak nerušeně krást data, šifrovat souboru, nebo krást výkon k těžení kryptoměn. Jedině tak si mohou zajistit nepřetržitou monetizaci.



Většina organizací si dobře chrání perimetr, ale už je slepá ve vnitřní síti. Protože žádná ochrana není 100%, a když dojde k prolomení perimetru, potřebujete nástroj, který dokáže detekovat pokročilé útoky na začátku a než dojde k větším škodám.

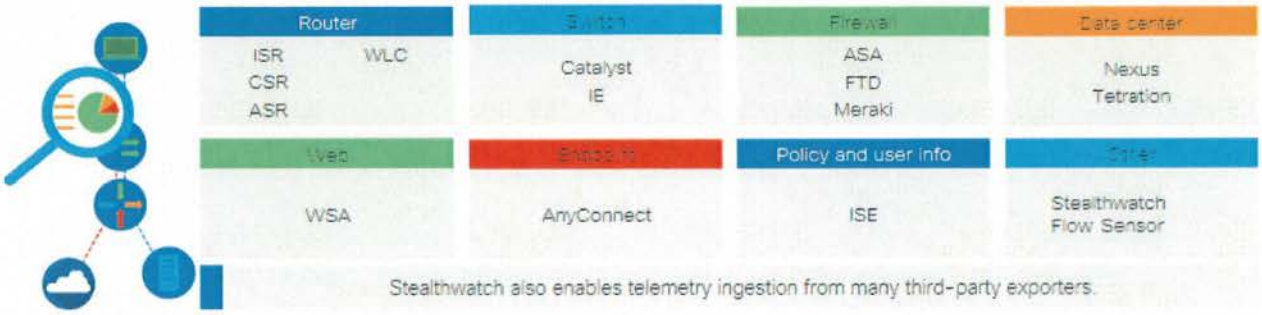
Cisco Stealthwatch poskytuje kontinuální viditelnost do veškerého síťového provozu. U každé IP adresy vytváří vzorek normální sítové aktivity a aplikuje k němu kontextovou analýzu k automatické detekci anomálií. Díky tomu umí Stealthwatch odhalit velkou řadu útoků včetně malware, zero-day, DDoS, advanced persistent threats (APTs), atp, ale i anomálie způsobené např. chybným nastavením.



Nyní s Cognitive Analytics můžete dokonce detekovat komunikaci malware v zašifrovaném provozu bez dekrypce na základě aplikace statistického modelu a strojového učení.

Telemetrická data můžete sbírat z nejen ze směrovačů, přepínačů, firewallů a sond, ale i z koncových zařízení a ISE. Díky tomu budete mít bohatá kontextuální data, ve kterých je

případně možno zpětně dohledat každou komunikaci, což může velmi pomoci např. při forenzní analýze.



ISR = Cisco Integrated Services Router; ASR = Cisco Aggregation Services Router; CSR = Cisco Cloud Services Router; WLC = Cisco Wireless LAN Controller; IE = Cisco Industrial Ethernet; ASA = Cisco Adaptive Security Appliance; FTD = Cisco Firepower® Threat Defense; WSA = Web Security Appliance; ISE = Identity Services Engine

Naše společnost Vám nabízí bohaté zkušenosti při nasazení Cisco Stealthwatch. Náš profesionální tým provede analýzu současného stavu a navrhne nejlepší možný scénář implementace a vyladí ji na míru. Následná podpora je pak samozřejmostí.

Nekupujte zajíce v pytli a požádejte si zdarma o vyzkoušení formou Proof of Concept (PoC)

Parametr číslo	**Požadovaná funkcionalita/vlastnost**	**Způsob splnění požadované funkcionality/vlastnosti**	**Nabídnul Dodavatel**
1	Celková kapacita systému (FPS, Flows per second) - min. 5000	ANO	ANO
2	**Flow kolektor**		
3	Požadovaný formát zařízení - HW appliance	ANO	ANO
4	Minimální počet zpracovaných toků za vteřinu (FPS, Flows per second) - 5000	ANO	ANO
5	Minimální počet síťových zařízení exportujících do jedné appliance pro sběr dat - 100	ANO	ANO
6	Sběr dat o datových tocích ze síťových zařízení	ANO	ANO
7	Baselining běžného provozu	ANO	ANO
8	Detekce anomálií oproti běžnému provozu i na L7	ANO	ANO
9	Detekce anomálií na základě toků v síti	ANO	ANO
10	Deduplikace záznamů o toku, pokud byl tentýž tok sebrán z více zařízení v síti	ANO	ANO
11	Spojení všech záznamů o toku, pokud se týkají té samé transakce mezi koncovými zařízeními	ANO	ANO
12	Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	ANO	ANO
13	Schopnost obohatit záznam toků o URL nebo uživatelskou aplikaci	ANO	ANO

14	Detekce úniku dat z organizace (Data Hoarding, Data Exfiltration)	ANO	ANO
15	Detekce šíření Malware	ANO	ANO
16	Detekce Botnetů	ANO	ANO
17	Detekce DDoS	ANO	ANO
18	Detekce scanu sítě	ANO	ANO
19	**Konzole pro správu a monitoring**		
20	Centrální správa flow kolektorů pro sběr a analýzu dat, případně dalších komponent systému, distribuovaných v síti	ANO	ANO
21	Možnost sběru dat/integrace s dalšími bezpečnostními prvky a systémy (firewall, web proxy, IDS/IPS, systémy řízení přístupu do sítě, ...)	ANO	ANO
22	Sběr dat a jejich prezentace z velkého množství rozdílných síťových segmentů současně (z distribuovaných appliancí)	ANO	ANO
23	Vizibilita napříč pevným i virtuálním prostředím	ANO	ANO
24	Detekce a prioritizace bezpečnostních hrozeb	ANO	ANO
25	Detekce porušení požadovaných politik	ANO	ANO
26	Pokročilé detekční techniky a detailní vhled do komunikační infrastruktury, aby byl využitelný pro detekci a obranu proti "Advanced Persistent Threats", malwaru, virů, síťových červů, cílených útoků, detekci DDoS útoků	ANO	ANO
27	Různé skupiny oznámení (alarmů)	ANO	ANO
28	Přehledové zobrazení všech oznámení (alarmů) na hlavní monitorovací obrazovce	ANO	ANO
29	Seskupování a grafická reprezentace vztahů a toků mezi logickými skupinami (definovanými uživatelem) komunikační infrastruktury	ANO	ANO
30	Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	ANO	ANO
31	Možnost napojení na centrální databázi hrozeb poskytovanou výrobcem, která je neustále aktualizovaná	ANO	ANO
32	Integrace se systémem řízení přístupu do sítě pro provádění automatizovaných nápravných akcí	ANO	ANO
33	Integrace se SIEM systémy	ANO	ANO
34	Funkcionality systému dostupné přes REST API	ANO	ANO
35	Implementace rozhraní pro sdílení informací s jinými bezpečnostními	ANO	ANO

	systémy - pxGrid nebo draft-ietf-mile-xmpp-grid-02		
36	Přístup administrátorů/uživatelů k systému podle uživatelských rolí/přístupových práv	ANO	ANO
37	Min. počet spravovaných flow kolektorů pro sběr a analýzu dat distribuovaných v síti - 20	ANO	ANO
38	Min. kapacita databáze pro historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu – 2TB	ANO	ANO

6. 802.1x

Cisco Identity Services Engine (ISE)

Popis navrhovaného řešení - Náhrada ACS + ověřování klientů LAN a WiFi pomocí 802.1X

- Ověřování přístupu uživatelů do LAN / WiFi pomocí 802.1X (Base License)
- Guest portál (Base License)
- Automatická profilace zařízení - IPT, kamera, WIFI AP, tiskárna,… (Plus licence)
- Posture – NAC (Apex licence)
- Propojení na další bezpečnostní systémy: FirePower, StealthWatch (Plus licence)
- + mnoho dalších doplňujících funkcí

Implementace 802.1x – minimální požadavky na funkcionalitu Cisco ISE Virtual Machine Small (p/n R-ISE-VMS-K9=)

Parametr číslo	Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Nabídnul Dodavatel
1	**Obecná charakteristika ověřovacího řešení**	ANO	ANO
2	Centralizovaný systém licencovaný pro 1000 uživatelů - pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)	ANO	ANO

3	Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup	ANO	ANO
4	Poskytuje AAA funkce (viz níže)	ANO	ANO
5	Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	ANO	ANO
6	Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity	ANO	ANO
7	Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	ANO	ANO
8	Dostupnost ve formě virtuální Appliance		ANO
9	Je dostupné ve formě Virtuálního stroje na platformách Vmware, Linux KVM a Microsoft Hyper-V	ANO	ANO
10	**AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)**	ANO	ANO
11	***Podporované protokoly***	ANO	ANO
12	RADIUS pro autentizaci, autorizaci, zaznamenávání	ANO	ANO
13	proxy funkce pro externí RADIUS	ANO	ANO
14	PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST	ANO	ANO
15	podpora TACACS+ pro centrální řízení administrativního přístupu na zařízení	ANO	ANO
16	Podporované databáze uživatelů (s možností definovat pořadí průchodu)	ANO	ANO
17	Interní (pro uživatele i koncová zařízení)	ANO	ANO
18	podpora vícero nezávislých Active Directory	ANO	ANO

19	LDAP (RFC 2251)	ANO	ANO
20	RADIUS Token indentity source (RFC 2865)	ANO	ANO
21	RSA RADIUS token server	ANO	ANO
22	Certifikační profil	ANO	ANO
23	Ověřování uživatelů a zařízení	ANO	ANO
24	Ověření uživatelů/zařízení heslem nebo certifikátem	ANO	ANO
25	Ověření MAC adresou připojovaného zařízení	ANO	ANO
26	Autorizace: pružný systém pro definici pravidel pro přístup k síti	ANO	ANO
27	Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:	ANO	ANO
28	uživatele (role, skupiny),	ANO	ANO
29	stavu a typu koncového zařízení (viz níže),	ANO	ANO
30	místa připojení,	ANO	ANO
31	historie připojení	ANO	ANO
32	Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO	ANO
33	Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	ANO	ANO
34	Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“	ANO	ANO
35	Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů	ANO	ANO
36	Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	ANO	ANO
37	Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat	ANO	ANO
38	Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)	ANO	ANO

39	Accounting	ANO	ANO
40	Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO	ANO
41	Dotazovací systém, korelace záznamů, centralizované výkazy	ANO	ANO
42	Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	ANO	ANO
43	Funkce GUEST serveru	ANO	ANO
44	Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	ANO	ANO
45	Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů	ANO	ANO
46	Samoobslužný portál pro uživatele	ANO	ANO
47	Ověření přes HTTP a HTTPS	ANO	ANO
48	Propojení s SMS bránou pro zasílání Guest účtu	ANO	ANO
49	Propojení s email serverem pro zasílání Guest účtu	ANO	ANO
50	Rozpoznávání typu koncových zařízení	ANO	ANO
51	Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	ANO	ANO
52	Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)	ANO	ANO
53	Předdefinované profily pro síťová zařízení NAD od různých vendorů	ANO	ANO
54	Podpora pro IPv6 koncová zařízení	ANO	ANO
55	Podpora BYOD	ANO	ANO
56	Onboarding (registrace, provisioning, nastavení klientských zařízení)	ANO	ANO
57	Onboarding/provisioning proces formou samoobsluhu	ANO	ANO

58	Specifické politiky pro BYOD zařízení	ANO	ANO
59	Možnost nastavení limitu BYOD zařízení pro jednoho uživatele	ANO	ANO
60	Interní CA, pro vydávání certifikátů BYOD zařízením	ANO	ANO
61	Interní CA lze řetězit jako subordinate pod firemní CA	ANO	ANO
62	Podpora MDM	ANO	ANO
63	Workflow pro registrace do MDM	ANO	ANO
64	Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant“)	ANO	ANO
65	Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení	ANO	ANO
66	Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení)	ANO	ANO
67	Rozpoznávání stavu koncových zařízení a jeho náprava	ANO	ANO
68	Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat:	ANO	ANO
69	instalovaný operační systém	ANO	ANO
70	opravy instalované v operačním systému	ANO	ANO
71	verze instalovaných programů	ANO	ANO
72	hodnoty položek v registry databázi systémů Windows	ANO	ANO
73	stav aplikací, zejména antivirů, antispyware, antimalware a firewall	ANO	ANO
74	Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)	ANO	ANO
75	Další vlastnosti	ANO	ANO
76	Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	ANO	ANO
77	Podpora SXP (Exchange Protocol) dle IETF	ANO	ANO
78	Otevřené API pro podporu propojení se zařízeními třetích stran	ANO	ANO
79	Upgrade současného ACS systému	ANO	ANO
80	Funkce pro správu ověřovacího	ANO	ANO

	systému		
81	Centralizovaná správa	ANO	ANO
82	Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	ANO	ANO
83	Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení	ANO	ANO
84	Grafické rozhraní pro definici pravidel přístupu k síti	ANO	ANO
85	Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	ANO	ANO
86	Diagnostika problemů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	ANO	ANO
87	Zaznamenávání událostí na externí syslog server	ANO	ANO
88	Podpora SNMPv3	ANO	ANO
89	NTP pro synchronizaci času	ANO	ANO
90	SMTP pro zasílání zpráv a výstrah přes e-mail	ANO	ANO

7. Podmínky propojení s ostatními prvky datacentra – použitá rozhraní

Celé řešení musí být dle schématu fyzického zapojení funkční jako celek a obsahovat potřebné transceivery/převodníky s respektováním následujících parametrů:

Parametr číslo	Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Nabídnul Dodavatel
1	**TYP č. 1**		
2	Rychlost modulu	10G	ANO, 10G
3	Typ modulu	SFP+	ANO, SFP+
4	Typ komunikačního rozhraní	Dual LC/PC	ANO, LC/PC
5	Použití	Ethernet komunikace	ANO, Ethernet
6	Vlnová délka	850nm	ANO, 850 nm
7	Typ optického vlákna	Více vidové	ANO, multi mode
8	Plná kompatibilita a podpora výrobcem přepínače	ANO	ANO, originální transceiver výrobce
9			
10	**TYP č. 2**		
11	Rychlost modulu	1G	ANO, 1G
12	Typ modulu	SFP	ANO, SFP

13	Použití	Ethernet komunikace	ANO, Ethernet
14	Typ komunikačního rozhraní	RJ-45	ANO, RJ-45
15	Plná kompatibilita a podpora výrobcem přepínače	ANO	ANO, originální transceiver výrobce
16			
17	**TYP č. 3**		
18	Rychlost modulu	10G	ANO, 10G
19	Typ modulu	SFP+	ANO, SFP+
20	Typ komunikačního rozhraní	Dual LC/PC	ANO, LC/PC
21	Použití	DWDM	ANO, DWDM
22	Vlnová délka	1558.98 nm	ANO, 1558.98
23	Plná kompatibilita a podpora výrobcem přepínače	ANO	ANO, originální transceiver výrobce
24			
25	**TYP č. 4**		
26	Rychlost modulu	10G	ANO, 10G
27	Typ modulu	SFP+	ANO, SFP+
28	Typ komunikačního rozhraní	Dual LC/PC	ANO, LC/PC
29	Použití	DWDM	ANO, DWDM
30	Vlnová délka	1558.17 nm	ANO, 1558.17
31	Plná kompatibilita a podpora výrobcem přepínače	ANO	ANO, originální transceiver výrobce

8. Jednotný management pro DC switching vrstvu a šifrátory

Jednotný management pro DC switching vrstvu a šifrátory Cisco Ent MGMT: Lic For PI 3.x And APIC EM Solution Apps (p/n R-MGMT3X-N-K9) - minimální požadavky na funkcionalitu

Na základě uvedených parametrů nabízíme řešení postavené na Cisco Prime Infrastructure 3.4 s příslušným počtem licencí pro šifrátory.

Parametr číslo	Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Nabídnul Dodavatel
1	Licence pro připravený virtuální obraz do virtualizovaného prostředí	ANO	ANO
2	Podpora Windows 2016 server & Hyper-V 2016 server, VMWare	ANO	ANO

3	Podporovaných síťových zařízení celkem	až 400	ANO
4	Dostatečný počet device licencí pro management datacentrových přepínačů, přepínačů pro out-of-band managment a šifrátorů	ANO	ANO
5	Podporovaných systémů pro víceúrovňový vhled a analýzu síťového provozu	4	ANO
6	Podporovaných fyzicky připojených klientů k aktivním prvkům	5500	ANO
7	Událostí zpracovaných za jednu sekundu celkem	100	ANO
8	Syslog zpráv zpracovaných za jednu sekundu	50	ANO
9	SNMP trapů zpracovaných za jednu sekundu	20	ANO
10	Systémových událostí zpracovaných za jednu sekundu	10	ANO
11	Zpracovaných toků Netflow - Netflow flow za sekundu	2500	ANO
12	Monitorovaných síťových rozhraní (polling)	2000	ANO
13	Platforma		ANO
14	Bezpečný přístup prostřednictvím webového grafického uživatelského rozhraní	ANO	ANO
15	Podpora autorizace a autentizace přístupu do systému vůči TACACS+	ANO	ANO
16	Podpora autorizace a autentizace přístupu do systému vůči RADIUS	ANO	ANO
17	Podpora řízení přístupu ke GUI pomocí identity (SSO - Single Sign On)	ANO	ANO
18	Podpora různých úrovní oprávnění pro přístup do systému (RBAC)	ANO	ANO
	Podpora multiuživatelského prostředí GUI s možností využít jak předdefinované skupiny, tak s možností definovat vlastní přístupová	ANO	ANO

19	oprávnění k funkcím GUI pro alespoň dvě uživatelské skupiny		
20	Podpora přístupu ke GUI z mobilních zařízení, např. tabletů	ANO	ANO
21	Podpora logování aktivity uživatelů a logování systémových událostí	ANO	ANO
22	Podpora zálohování systému a obnovy ze zálohy	ANO	ANO
23	Možnost změnit nastavení doby ukládání historických a agregovaných dat	ANO	ANO
24	Možnost omezit přístup uživatelům pouze ke skupině zařízení, např. na základě lokality, typů zařízení apod.	ANO	ANO
25	Možnost monitoringu provozních parametrů aplikací	ANO	ANO
26	Možnost zpracování informací o provozu v síti (NetFlow) včetně deduplikace dat z více zdrojů	ANO	ANO
27	Možnost zobrazit informace o chování aplikací v síti (statistiky, identifikace případných problémů na síťové nebo aplikační úrovni, zhoršení uživatelské zkušenosti uživatelů)	ANO	ANO
28	Podpora protokolu IPv4	ANO	ANO
29	Podpora protokolu IPv6	ANO	ANO
30	Podpora protokolu SSH	ANO	ANO
31	Podpora protokolů SNMPv1, SNMPv2, SNMPv2c a SNMPv3	ANO	ANO
32	Podpora zpracování SYSLOG zpráv	ANO	ANO

33	Podpora zpracování SNMP zpráv	ANO	ANO
34	Možnost úpravy zpracování událostí a alarmů včetně např. potlačení vybraných alarmů	ANO	ANO
35	Možnost kategorizace alarmů a událostí	ANO	ANO
36	Možnost nastavit zasílání upozornění na vybrané události emailem	ANO	ANO
37	Podpora MIB třetích stran	ANO	ANO
38	Možnost monitoringu parametrů definovaných v MIB třetích stran	ANO	ANO
39	Možnost definovat vlastní události na základě SNMP nebo SYSLOG zpráv	ANO	ANO
40	Možnost exportu zpráva a událostí	ANO	ANO
41	Možnost generovat zprávy pro nadřazený management systém	ANO	ANO
42	Posílání alarmů a událostí network management aplikacím třetích stran, které podporují FCAPS	ANO	ANO
43	Podpora API pro programatický přístup k funkcionalitě aplikace správy	ANO	ANO
44	Schopnost management systému nalézt automaticky zařízení v síti s využitím více různých metod pracujících s informacemi z druhé a třetí vrstvy	ANO	ANO
45	Schopnost management systému filtrovat nalezená zařízení – vyloučit resp zahrnout definované adresní rozsahy	ANO	ANO

46	Schopnost management systému připravit konfigurační a jiné změny formou úlohy včetně schvalovacích mechanizmů	ANO	ANO
47	Podpora pro vyhledávání informací o síťových zařízení, připojených koncových zařízení, uživatelích, konfigurovaných parametrech, alarmech, událostech apod. napříč celým management systémem.	ANO	ANO
48	Správa aktivních prvků	ANO	ANO
49	Požadavky na škálování - systém musí být schopen kromě LAN / WAN sítě spravovat a monitorovat také bezdrátovou síť pouhým přidáním příslušných licencí	ANO	ANO
50	Kompletní správa životního cyklu LAN / WAN sítě (plánování, nasazení, monitoring, troubleshooting, reporting)	ANO	ANO
51	Inventarizace HW síťových prvků	ANO	ANO
52	Inventarizace, nasazení a správa firmware aktivních prvků	ANO	ANO
53	Analýza vhodnosti firmware aktivních prvků pro nasazení	ANO	ANO
54	Generování reportů inventory aktivních prvků	ANO	ANO
55	Konfigurace pomocí šablon pro zefektivnění konfiguračních úloh	ANO	ANO
56	Inventarizace, verzování, archivace a správa konfigurací LAN/WAN sítě	ANO	ANO

57	Předpřipravené šablony dle doporučení výrobce - "best practice"	ANO	ANO
58	Možnost udržovat konfigurace v souladu se standardem Zadavatele, identifikovat neshody	ANO	ANO
59	Celkové konfigurační šablony sestavovány z dílčích šablon konfigurací jednotlivých funkcí nebo uživatelsky definovaných konfigurací jednotlivých funkcí	ANO	ANO
60	Podpora pro automatizovanou konfiguraci nově připojovaných zařízení	ANO	ANO
61	Zobrazování alarmů a událostí z LAN / WAN sítě	ANO	ANO
62	Topologická mapa	ANO	ANO
63	Nástroje pro detekci a řešení problémů v LAN / WAN síti	ANO	ANO
64	Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souhrnném pohledu (kontextově) pro rychlejší troubleshootnig	ANO	ANO
65	Zobrazení informací o uživateli, koncovém či síťovém zařízení v kontextu informací souvisejících s jeho okolím a provozními parametry	ANO	ANO
66	Detailní monitoring LAN / WAN sítě	ANO	ANO
67	Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí	ANO	ANO
68	Monitorování výskytu koncových zařízení a uživatelů v síti	ANO	ANO

69	Monitoring a vyhodnocování přenosových parametrů z NetFlow	ANO	ANO
70	Monitoring funkčnosti (včetně odezev) přenášených aplikací	ANO	ANO
71	Monitoring parametrů zdraví aktivních prvků a jejich přehledné zobrazení	ANO	ANO
72	Možnost nastavit prahové hodnoty pro monitoring parametrů zdraví aktivních prvků	ANO	ANO
73	Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí	ANO	ANO

9. Podmínky záručního servisu

(1) Záruční doba bude činit minimálně 72 měsíců a začne běžet dnem podpisu Celkového akceptačního protokolu – tj. po dodání všech zařízení a provedení instalací, kde je to stanoveno.

(2) Vyřešení závady nejpozději do konce pracovního dne, následujícího po dni nahlášení závady (Fix time – NBD on-site). Response time 2 hod od nahlášení[1].

(3) Jediné objednávkové místo servisních zásahů pro všechna zařízení i jejich součásti.

(4) Propojení helpdesku Objednatele a Dodavatele do 3 měsíců po podpisu smlouvy. V helpdeskovém systému se budou automaticky přenášet minimálně tyto informace:
   a. datum a čas nahlášení požadavku
   b. lokalita
   c. popis požadavku
   d. kontaktní osoba
   e. potvrzení o přijetí požadavku
   f. jméno řešitele
   g. datum a čas vyřešení
   h. poznámky

(5) Dostupnost servisu v pracovní dny od 6.00 do 18.00.

(6) Záruka se bude vztahovat na technická zařízení a všechny jejich dílčí komponenty.

(7) Dodavatel poskytne Objednateli po dobu trvání záručního servisu všechny relevantní SW releases a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad.

[1] Tj. Pokud je požadavek nahlášen v pondělí ve 13:00, musí být závada vyřešena do úterý 18:00.

(8) Dodavatel se zavazuje informovat Objednatele o nových verzích SW a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který Objednatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Dodavatel se zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.

(9) Dodavatel je povinen zajistit Objednateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.

(10) Objednatel musí mít možnost se sám zaregistrovat na stránkách výrobce a musí mít možnost samostatného stahování nových verzí SW a registrace k odběru automatických mailových zpráv týkajících se dodávaných zařízení a upozorňující na tyto skutečnosti:

- bezpečnostní incidenty, které vyžadují od Objednatele povýšení operačního systému/firmware či aplikování změny konfigurace či záplaty,
- konec prodeje či podpory,
- nové verze operačního systému/firmware
- známé chyby operačního systému/firmware

(11) Objednatel poskytne Dodavateli omezený přístup do sítě prostřednictvím sondy – serveru, který si Dodavatel nainstaluje a prostřednictvím něj bude spravovat dodaná zařízení. Tato sonda bude zajišťovat automaticky funkce uvedené v předchozím odstavci.

(12) Dodavatel bude používat výhradně nové, originální díly určené pro evropský trh (Dodavatel může být Objednatelem průběhu plnění požádán o předložení potvrzení výrobce resp. distributora v tomto smyslu).

(13) Záruční servis bude zajišťován přímo Dodavatelem nebo prostřednictvím jeho partnerské servisní organizace v datových centrech ČÚZK. Za kvalitu a včasnost provádění servisu ručí vždy Dodavatel.

(14) Veškeré náklady servisu, s výjimkou nákladů na servisní zásahy vyvolané neodbornou manipulací pracovníků Objednatele s instalovaným zařízením a nákladů na zbytečný výjezd servisních pracovníků, jsou součástí nabídkové ceny Dodavatele.

(15) Servisní zásahy budou přednostně prováděny v místě instalace zařízení a mohou probíhat i výměnným způsobem. Závada, jejíž odstranění z jakýchkoliv důvodů nebude na místě možné, bude řešena výměnným způsobem. Jestliže dojde k opravě, bude původní zařízení po opravě navráceno uživateli. Veškerá manipulace s opravovaným zařízením bude protokolárně zaznamenána. V případě, že oprava vadného zařízení nebude možná, bude předmětné zařízení nahrazeno novým stejných nebo lepších parametrů, na němž bude možno provozovat stejný SW jako na původním.

(16) Komunikace bude probíhat výhradně v českém či slovenském jazyce.