PŘÍLOHA č. 1

TECHNICKÁ SPECIFIKACE

Tato příloha je nedílnou součástí zadávací dokumentace veřejné zakázky s názvem

„Bezpečné síťové prostředí "

Obsahuje podrobné vymezení předmětu veřejné zakázky. Požadavky specifikované v přiložených tabulkách této přílohy považuje Zadavatel za minimální a na jejich splnění Zadavatel trvá.

Předmět veřejné zakázky se skládá z následujících částí:

1. Vypracování Detailního návrhu řešení,
2. Dodávka technologií Bezpečného síťového prostředí,
3. Instalace a implementace Bezpečného síťového prostředí,
4. Služby úpravy konfigurací současných bezpečnostní technologií,
5. Poskytnutí služeb podpory výrobců technologie, dle skupin produktů, na 3 a 4 roky od ukončení Instalace a implementace,
6. Poskytnutí školení a servisní podpory spojené s provozem technologie
7. Poskytování dalších odborných služeb

Dílo bude realizováno a předáváno po etapách. Etapy vycházejí z hrubého harmonogramu, které jsou uvedeny v čl. 7 této přílohy ZD. Začátek každé etapy je vázán na protokolární převzetí předchozí etapy Zadavatelem na základě akceptačního protokolu.

Obsah

1. Vypracování Detailního návrhu řešení

Dodavatel samostatně vypracuje do 6 týdnů od podpisu smlouvy Detailní návrh řešení.

Detailní návrh řešení bude obsahovat minimálně členění na tyto kapitoly:

- Místní šetření - detailní analýza ve všech dotčených lokalitách
- Zpracování High-Level a Low-level designu síťové topologie
- Vytvoření prováděcího projektu, projektové přípravy a návrh dohodnutí součinností
- Předložení Detailního návrhu řešení Zadavateli

Detailní návrh řešení bude vypracován ve dvou etapách 1 a 2.

Etapa č. 1 - Místní šetření

1. Analýza - místní šetření - ve všech dotčených lokalitách s cílem zjistit všechny detailní informace potřebné pro vypracování prováděcího projektu.
2. Specifikace hardware, který bude součástí dodávky řešení
3. Vytvoření prováděcího projektu, Projektová příprava, dohodnutí součinností, apod.
4. Budou provedeny workshopy s garanty navazujících částí infrastruktury MHMP (servery, bezpečnost, aplikace, ...) s cílem definovat vzájemné vazby a identifikovat rizika migrace. Zjištěné informace budou zaneseny do prováděcího projektu v rámci etapy č. 2.
5. Zkreslení tzv. High-Design and Low-Design sítě
6. Specifikace požadavků na provozní prostředí, např. mohou být identifikovány potřeby nutné pro realizaci migrace (zajištění napájení, místa v racích apod.)

Etapa č. 2 - Prováděcí projekt

V rámci této části bude upřesněn detail ohledně umístění a nastavení jednotlivých zařízení. Bude se jednat primárně o definici a popsání následujících údajů:

7. přesné rozmístění jednotlivých zařízení
8. stanovení způsobu propojení zařízení až na úroveň konkrétních portů, IP adres, konektorů apod.
9. vytvoření migračního plánu pro každý funkční blok síťové infrastruktury
10. definování garantů v jednotlivých lokalitách a stanovení klíčových uživatelů pro ověřování funkčnosti systémů
11. pojmenování dopadů do stávající infrastruktury (rekonfigurace serverů, aplikací, operátorských linek, Mepnetu apod.) a zajištění součinnosti jejich správců
12. bude vytvořen/aktualizován IP adresní plán, stanoveny jmenné konvence apod.
13. bude staven způsob distribuce IP směrovacích záznamů pro interní sítě MHMP, pro perimetr MHMP, pro Mepnet lokality
14. budou definovány komunikační pravidla pro nastavení firewallů
15. budou definovány bezpečnostní politiky pro zabezpečení komunikačních linek (IPSec, 802.3ad)
16. budou definovány požadavky na součinnost externích subjektů

17. vytvoření postupu migrace pro stávající zařízení, které budou dále využity (Catalyst 6500, linkové karty, SFP/SFP+ moduly apod.)
18. bude zapracován projekt k vytvoření řešení vizualizace a definice vztahů IT aktiv a služeb organizace, kde výstupem bude řešení v jednotné uživatelské správě přes GUI:
    - Správu IP adresního plánu organizace
    - Provoz a podpora služeb DNS a DHCP
    - Řízení přístupu do sítě v rozsahu nástrojů:
    - Network Access Control (NAC)
    - SSL VPN
    - Monitoring chování sítě pro úrovně L2, L3 a L4
    - Vizualizace vztahů IT aktiv a provozovaných služeb organizace
    - Evidence popisných informací IT aktiv pro podporu šetření bezpečnostních událostí
    - Modelování logických vrstev pro definici vztahů klíčových procesů organizace na IT aktiva
19. bude zpracován projekt k vytvoření kompletní přehled nad síťovým provozem a jeho inteligentní distribuci a předzpracování předtím než dorazí na monitorovacích nástrojů (např. IPS/IDS, SIEM, DLP, APM, apod.). Dodaným řešením zajištěn přehled nad veškerým síťovým provozem - vhled do fyzických (včetně vzdálených lokalit) i virtuálních sítí.
20. Bude zpracován návrh integrace s ostatními bezpečnostními systémy provozovanými nebo využívanými Zadavatelem, které budou umožňovat napojení na Bezpečné síťové prostředí
    - Perimetrové firewally společnosti
    - Systémy řízení a sledování přístupů k síti, DDI a Network Visibility Module
    - Systémy aplikačního balancování a ochrany
    - Systém správy logů z provozní a bezpečnostní infrastruktury
    - Nástroje pro detekci a vyšetřování kybernetických incidentů
    - Nástroje pro správu bezpečnostních událostí SIEM
21. Stanovení základních kategorií dat pro směrování do výše uvedených systémů - bezpečnostní log data, log data s vlivem na služby, log data s vlivem na aplikace, log data s vlivem na systémy.
22. Detailní popis implementace, včetně časového harmonogramu
23. Popis instalačních procedur
24. Návrh akceptačních kritérií pro předání díla, včetně návrhu akceptačního protokolu pro předání díla do provozu

Detailní návrh bude podroben interní oponentuře Zadavatele. V případě připomínek Zadavatele je Dodavatel povinen tyto připomínky do detailního návrhu řešení zapracovat. Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky. Detailní návrh řešení se stane jeho předáním majetkem Zadavatele, který jej bude moci plně využít pro svoje potřeby ke všem způsobům užití, a to bez dalšího souhlasu zhotovitele nebo zpracovatele.

2. Dodávka technologií Bezpečného síťového prostředí

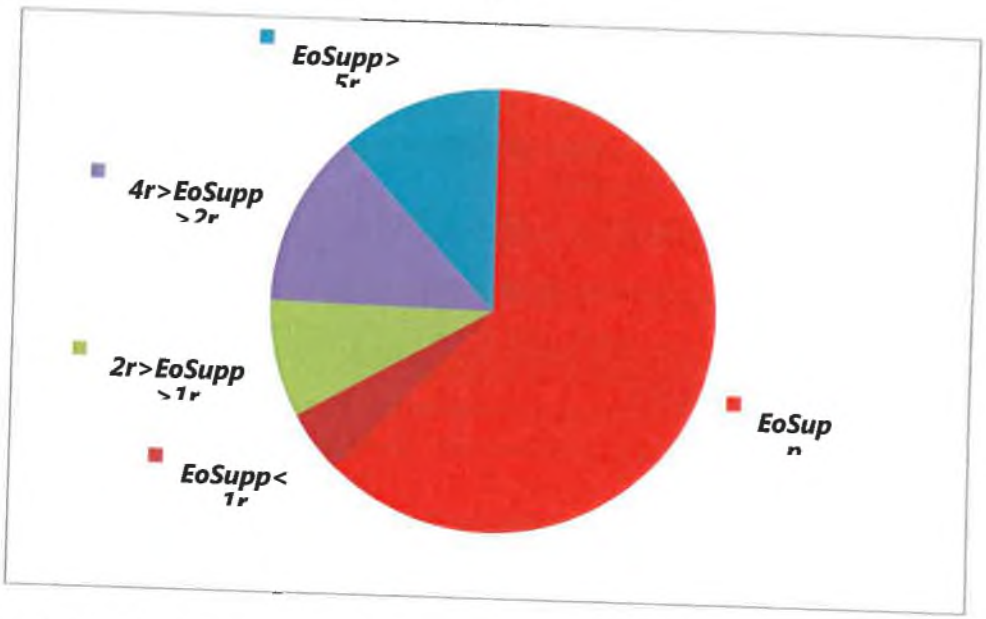
POPIS STÁVAJÍCICHO STAVU

Infrastruktura MHMP je rozložena ve 21 lokalitách. Centrálními lokalitami jsou lokality DC1 a NUB, které jsou vzájmenně propojeny MPLS Interconnect sítí prostřednictvím koncových MPLS zařízení Juniper MX240.

Lokality VAL, STAR, REZ, KLA, MKP, JUN a NR jsou fyzicky připojeny optickými vlákny napřímo (mimo MPLS WAN) na jednu z centrálních lokalit - NUB. Lokality JUN a NR jsou připojeny Single Mode (SM) optikou. Ostatní lokality jsou na centrální lokalitu NUB připojeny Multi Mode optikou (MM). U zbylých 12 lokalit MHMP (BOH, BREV, BUB, DŮM, CHAR, JAR, EMA, KON, OPLET, RAB, RYT, VYS) je konektivita na centrální lokality zajištěna prostřednictvím MPLS sítě WAN, která je připojena do MPLS Interconnect sítě, propojující centrální lokality (DC1 a NUB).

Vnitřní infrastruktura jednotlivých lokalit se typicky liší podle její velikosti. Malé lokality, kterých je většina, jako jsou např. VYS, VAL, STAR, RYT, REZ, OPLET, MKP, CHAR, JAR, BOH jsou vybaveny malým počtem L2 switchů bez zajištěné vysoké dostupnosti (redundance zařízení a fyzických propojů). Centrální lokality DC1, NUB a větší lokality JUN, NR, KON jsou kromě přístupových L2 switchů vybaveny redundantními L3 switchi, které zajišťují L3 routing již v rámci své lokality. Výjimkou je jedna z menších lokalit EMA, která je rovněž vybavena L3 switchem, který zajišťuje pro lokalitu Inter-VLAN routing. Tento L3 switch ovšem rovněž není v redundantním zapojení pro zajištění vysoké dostupnosti.

Celkový počet stávajích aktivních prvků je **304.**



Obrázek 1 Statistika dostupnosti technické podpory od výrobce (EOS)

Z analýzy typů síťových prvků používaných v infrastruktuře MHMP vyplývá, že pro 62% (189ks) zařízení již neexistuje žádná dostupná technická podpora pro případ jakéhokoliv problému v hardwaru nebo v software (EoSupp). Dalších 5% (14ks) zařízení je těsně před koncem dostupnosti podpory resp. podpora bude dostupná již jen několik měsíců (EoSupp<1r). Pro 9% (26ks) zařízení bude podpora k dispozici po dobu kratší než 2roky (2r>EoSupp>1r). Pro 13% (39 zařízení) zařízení bude technická podpora dostupná po následující 2 až 4 roky (4r>EoSupp>2r). V případě, že dostupnost technické podpory je kratší než 5 let, to znamená, že již byly dovršeny termíny pro morální životnost zařízení (End of Life) a ukončen prodej takových zařízení (End of Sale). Z analýzy používaných zařízení plyne, že 88% (268ks) zařízení je již za hranicí své morální životnosti. Pouze v případě 12% (36ks) zařízení z celkového počtu 304 kusů je možné tyto zařízení považovat z hlediska jejich

životnosti za vyhovující.

REDUNDANCE

Prakticky v žádné z 21 lokalit není zajištěna potřebná úroveň redundance síťových zařízení a tedy vyhovující vysoká dostupnost (HA).

Ve většině případů lokality nedisponují dvojicí redundantních páteřních prvků. Pokud takové prvky v lokalitě existují (např. DC1, NUB, KON), nejsou tyto prvky v HA režimu provozovány. To znamená, že na prvcích, které podporují vytváření stohu switchů, kdy se z více jednotlivých switchů (Catalyst 2960S, 2960X, 3750, 3750X) vytvoří jeden fyzický switch propojený na úrovni vnitřních sběrnic nebo na prvcích, které umožňují propojení prostřednictvím 10GE rozhraní do virtuálních chassis (VSS), který se opět chová jako jeden fyzický switch, těchto vlastnosti nevyužívá (nebo nejsou takové HA vlastnosti na switchích vůbec dostupné. Takové stohy nebo virtuální chassis lze efektivně propojovat s dalšími switchi případně servery prostřednictvím agregovaných (EtherChannel 802.3ad) Ethernet propojů bez nutnosti vytvářet v síti zbytečné smyčky a provozovat, mimo nezbytnou míru, protokol SPT (Spanning Tree Protocol), který vykazuje nedostatečnou konvergenci sítě v případě výpadků a poruch na síti.

Hlavní nedostatky:

- Nedostatečná redundance páteřních nebo centrálních prvků (stack/stoh, VSS).
- Pouze v minimální míře se využívá agregace fyzických propojů do vícenásobných tras (802.3ad).
- Prakticky se nevyužívá agregací (802.3ad) fyzických tras a jejich zapojení do různých prvků jednoho redundantního uzlu (protože takové redundantní uzly neexistují).
- Nevyužívá se rozložení zátěže mezi přenosové trasy a síťové prvky (také z důvodů uvedených v předchozích bodech).
- Riziko výpadků v síti v důsledku poruch nezálohovaných fyzických komponent sítě.
- Riziko výpadků v síti v důsledku pomalé nebo chybové konvergence sítě postavené na SPT protokolu.
- V souvislosti z výše uvedenými body vyplývá nemožnost zajištění redundantního napájení klíčových uzlů sítě.

BEZPEČNOST

Hlavní nedostatky:

- Nejednotná koncepce architektury vyplývající z postupné výstavby sítě v dlouhém časovém horizontu.
- Komplikovaná správa takové infrastruktury.
- Z důvodu morální zastaralosti některých klíčových bezpečnostních prvků vyřazeny klíčové bezpečnostní služby
- Chybějící kontrolér pro řízení přístupu k aplikacím a dělením zátěže na serverové farmy (původní ACE).
- Systém pro monitoring, sběr, korelaci a vyhodnocování bezpečnostních událostí (původní MARS 55).
- Výchozí brány pro lokální sítě jednotlivých lokalit nejsou ve správě MHMP (PE zařízení MPLS sítě WAN).
- Na switchích chybí řízení oprávnění konektivity koncových zařízení k LAN sítím MHMP - chybějící 802.1X.

- Datové přes veřejné MPLS sítě nejsou šifrovány.

Požadavek na cílový stav projektu

1. Veškerá stávající zařízení po době morální životnosti budou nahrazena
2. Zařízení a komponenty, které vyhovují funkčně a budou v horizontu min. 5 let podporovány výrobcem, budou dále využity. Tímto způsobem budou maximálně zužitkovány vynaložené investice MHMP
3. Z pohledu počtu připojených zařízení nebude v cílovém stavu docházet k zásadnímu navýšení
4. V klíčových bodech sítě bude v maximální možné míře použito redundantních mechanismů
5. Dojde ke změnám ve prospěch navýšení bezpečnosti přenášených dat. Tímto lze předejít negativním bezpečnostním nálezům v rámci analýzy rizik (např. v rámci nových legislativních požadavků – GDPR)
6. Dojde k zavedení ověřování zařízení připojujících se k lokální síti
7. Budou použity analytické nástroje pro detekci konkrétních aplikaci a škodlivého kódu v síťovém provozu
8. Bude nasazen nástroj pro centrální řízení a správu síťových politik

Očekávané přínosy řešení

9. Bezpečnostní přínosy plynoucí z analýzy síťového provozu:
    - Monitoring bezpečnosti – detekce provozu porušující bezpečnostní politiky, anomálie, šíření škodlivého kódu. Včetně monitoringu každého přenášeného paketu umožňují- cího detekovat i útoky vedené proti organizaci.
    - Detekce šíření škodlivého kódu i v šifrovaném provozu, bez porušování utajení provozu šifrou
    - Utajení šifrováním veškerého provozu v infrastruktuře mezi všemi prvky a budovami, zejména v částech sítě, které nejsou fyzicky zabezpečeny nebo jsou snadněji fyzicky přístupná či nejsou zcela pod kontrolou organizace. Vysoce propustnou a bezpečnou technologií IEEE 802.1ae, která však přesto umožňuje plně využívat veškeré síťové funkce zařízení.
10. Nezávislost na poskytovateli
    - Vlastní překryvná VPN síť přináší nezávislost na poskytovateli MAN připojení
    - Umožňuje rovněž zřídit záložní přípojky u nezávislého poskytovatele
11. Viditelnost aplikací

    Zařízení používají vhled do vyšších vrstev OSI modelu pro rozpoznání přenášené aplikace. Tuto znalost následně využívají při uplatnění bezpečnostních nebo i QoS pravidel podle detekované aplikace. Současně poskytují i telemetrická data kategorizovaná podle přenášených aplikací
12. Telemetrie, programovatelnost/automatizace

    Pro zjednodušení správy řešení a automatizaci rutinních úkonů obsahují zařízení programovatelná rozhraní jak pro vlastní ovládání zařízení tak i pro automatizovaný a vysoce škálovatelný (autonomní) sběr požadovaných telemetrických dat
13. Vysoka dostupnost (Modulární OS, patching)

    Moderní zařízení s moderní architekturou operačního systému zaměřenou

na dosažení vysoké dostupnosti zařízení a jím poskytovaných služeb (dříve dostupnou pouze u zařízení určených pro poskytovatele služeb)

14. SDA Fabric

V řešení použitá zařízení umožňují vytvoření tzv. "fabriky", tedy sítě ovládané primárně pomocí politik. Pomocí vyjádření záměru, kterého je potřeba dosáhnout, nikoli konfiguračními změnami konkrétních zařízení. Takovýto přístup k řízení sítě přináší velmi jednoduchým způsobem vytvořitelnou, vysoce bezpečnou a velmi škálovatelnou segmentaci (bezpečnostní oddělení segmentů, virtualizaci) celé infrastruktury, zabezpe- čení a řízení přístupu do sítě, monitoring provozních parametrů a telemetrická data. Segmentace je prováděna na základě identity koncového uživatele, nikoli jeho síťových parametrů, což umožňuje vysokou škálovatelnost, flexibilitu i při častých nebo dočas- ných změnách uspořádání koncových uživatelů infrastruktury, jejich mobilitu. Není potřeba žádný manuální zásah do infrastruktury, a přesto jsou zachovány veškeré politiky všech uživatelů. Telemetrická data z provozu infrastruktury pro jejich analytické zpracování do údajů relevantních pro primární předmět podnikání společnosti nebo chod organizace. Obecně tento přístup zefektivňuje zavádění nových služeb infrastruktury a řešení problémů a úkolů.

Předpokládá se využití filosofického směru, který byl v prostředí MHMP zvolen v nových DC (např. DC4, DC2). Jedná se o technologii **SDN – software defined network**. V tomto prostředí již datové toky nejsou za všech okolností řízeny tradičním způsobem, ale mohou být ovládány softwarově na základě schopnost specificky zacházet s provozem dle příslušnosti k jednotlivým aplikacím.

Seznam technologických celků dodávky Bezpečné síťové prostředí

Předpokládané rozdělení objemu dodávky v jednotkách kusů, dle Přílohy č. 5: Podrobná specifikace ceny, Smlouvy, na jednotlivé fáze.

Součástí Detailního návrhu řešení může být úprava množství technologií, dodaného v jednotlivých fází, avšak celkový počet technologií nesmí být pozměněn.

Technologie	Fáze 1	Fáze 2
- Bezpečné rozhraní pro analýzu síťového provozu	0	4
- Bezpečnostní hraniční brány firewall pro sítě Mepnet	5	0
- Centrální kontrolér LAN sítě	3	0
- Monitorování datových toků	0	1
- Řízení přístupu k síťovým prostředkům (802.1x)	2	2
- Správa síťového prostředí	0	1
- Datacentrové řešení Spine-Leaf	1	0
- Spine vrstva	2	0
- Leaf vrstva – 10GB SFP+	4	0
- Leaf vrstva 10GB – RJ45	2	0
- Leaf vrstva 1GB – RJ45	10	0
- Next-Generation Firewall	2	0
- Virtuální privátní sítě, vzdálené přístupy do sítě	5300	0
- Přístupové přepínače s 24 PoE porty	30	50
- Distribuční přepínače	30	43
- Přístupové přepínače s 48 PoE porty	32	40
- Centrální přepínače	3	3
- Agregační směrovač	0	2
- Hraniční pobočkové směrovače	4	2
- Rozšiřující 10GB karty	3	0
- Rozšiřující servisní moduly	4	0
- Propojovací moduly	200	143
Podrobné specifikace a parametry technologií jsou popsány v následující kapitole této přílohy ZD		

Pravidla pro vyplňování technických parametrů řešení

Uchazeč vyplní v následujících kapitolách pouze všechny žlutě označené části.

Tato příloha slouží k uvedení názvu / typu a počtu konkrétního nabízeného řešení či zařízení a dále **k vymezení minimálních technických požadavků zadavatele na řešení a osvědčení jejich splnění uchazečem**. Požadavky zadavatele jsou uvedeny ve sloupci „Paramater" nebo „Požadovaná hodnota paramateru".

Následná smlouva s vybraným uchazečem může být v této části upravena tak, aby obsahovala již pouze uchazečem nabídnuté zařízení a jeho technické parametry.

V níže uvedených tabulkách jsou uvedeny veškeré povinné minimální parametry kladené na celý systém. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Splňuje ANO/NE" a pokud je požadován i „Popis jak bude požadavek splněn/řešen".

Sloupec vyjádření „Splňuje ANO/NE" může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Sloupec „Nabízená hodnota (Popis)" bude obsahovat podrobný popis, jak dodavatel požadavek naplní.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

Výše uvedená pravidla na vyplnění tabulek jsou společné pro všechny kapitoly této přílohy ZD.

2.1. Bezpečné rozhraní pro analýzu síťového provozu

Technické požadavky na řešení garantovaného a bezpečného rozhraní pro analýzu síťového provozu.

Systém musí poskytovat funkcionality umožňující vytvoření bezpečného rozhraní mezi síťovými prvky nové infrastruktury DC MHMP a provozně bezpečnostními nástroji, které vyžadují čtení kopírovaného síťového provozu. Takto vytvořené bezpečné předávací rozhraní (jinými slovy integrační platforma pro síťě – neboli packet broker) bude sloužit k předávání informací o síti a ze sítě, které bude možno bezpečně a bez dalších nároků na síť (tedy bez ohrožení její stability) využív v nástrojích třetích stran.
Zdroje dat k monitoringu je třeba zajistit také z virtualizační platformy VMware, tedy z virtuálních síťových přepínačů, které jsou zajištěny na úrovni hypervizorů virtuálního prostředí.

Předávací rozhraní síťového provozu musí být dále vybaveno možnostmi manipulace s předávanými informacemi, čímž bude umožněno např. filtrování vybraného typu provozu k odeslání do zařízení třetích stran, nebo maskování citlivého obsahu, aby nemohlo dojít k jeho vyzrazení a neoprávněnému nakládání.

Minimálně je požadováno posktynutí těchto parametrů a pokrytí těchto oblastí:

- Schopnost připojit dodávané řešení až na 40 x 10GE RJ45 metalických rozhraní, nebo až na 40 x 10GE optických rozhraní
- Schopnost připojit dodávané řešení až na 40 x 1GE RJ45 metalických rozhraní, nebo až na 40 x 1GE optických rozhraní
- Schopnost připojit dodávané řešení až na 2 x 40GE optických rozhraní, nebo až na 2 x 100GE optických rozhraní
- Schopnost agregovat a zpracovat celkem 100 Gbps síťového provozu
- Podpora těchto způsobů integrace s monitorovanou sítí:
    - SPAN/MIRROR port – připojení na optické či metalické rozhraní síťových přepínačů, které jsou nastaveny do režimu duplikace provozu pro monitoring
    - Možnost rozšíření řešení o režim TAP – síťový rozbočovač pro optické a metalické sítě
- Agregace provozu z více zdrojů do jednoho výstupního rozhraní a média
- Podpora sledování sítového provozu ze síťového přepínače hypervizoru VMware
- Schopnost sledovat provoz v 10 serverech VMware virtuálního prostředí HMP
- Možnost řízení pravidel směrování monitorovaného provozu, kde je možné libovolným odběrným místům přidělit konkrétní zdrojová data ze sledovaného síťového provozu
- Možnost manipulace s daty z monitorovaného provozu, předtím než dojde k jejich předání odběrnímu místu
- Možnost deduplikovat a optimalizovat provoz předávaný odběrným místům
    - Možnost předávat unikátní informace i přesto, že na vstupu přichází z několika zdrojů současně (deduplikace)

- Možnost předávat omezené informace o síťovém provozu: jen NetFlow, nebo jen hlavičky provozu bez obsahu
- Možnost upravovat výstupní data obohacením o dodatečné informace

Tabulka detailních požadavků na dodávané řešení garantovaného a bezpečného rozhraní pro analýzu síťového provozu:

☐ Základní údaje	Nabízená hodnota
Výrobce zařízení	Gigamon
Počet kusů zařízení - 4	4
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	GVS-HC301 GVS-TAX01
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.gigamon.com/content/dam/resource-library/english/data-sheet/ds-gigavue-hc3.pdf https://www.gigamon.com/content/dam/resource-library/english/data-sheet/ds-gigavue-ta-series-traffic-aggregation.pdf

Parametr	Požadovaná hodnota parametru (pro jedno fyzické zařízení)	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Integrace s monitorovaným síťovým prostředím	Analýza síťového provozu probíhá pro veškerý síťový provoz a bez ohledu na použité komunikační protokoly a monitorovány jsou tedy všechny probíhající spojení na všech síťových portech monitorované infrastruktury.	Technologie analyzuje veškerý provoz z připojených rozhraní sítě a proto disponuje dostatečným množstvím a kapacitou vstupních síťových rozhraní. Technologie nerozlišuje provoz na vstupních rozhraních a zpracovává veškerá zaslaná data.	ANO
Integrace s monitorovaným síťovým prostředím	Integrace se síťovým prostředím je zajištěna zrcadleným síťovým provozem, který Zadavatel poskytne na vyhrazených portech přepínačů svých DC.	Data jsou primárně do nabízené technologie sbírána ze SPAN rozhraní monitorované	ANO

		síťové infrastruktury. Přičemž SPAN porty zajišťuje síťové prostředí zákazníka.	
Integrace s monitorovaným síťovým prostředím	Pro integraci s monitorovanou sítí bude možné použít kombinaci metalických a optických sítových rozhraní DC Zadavatele.	Navrhované řešení disponuje kombinací rozhraní 1Gbps metalické a 10, 40Gbps optické.	ANO
Integrace s monitorovaným síťovým prostředím	Bude možné rozšířit řešení o in-line způsobu zapojení pro metalické i optické komunikační trasy pomocí TAP.	Nabízené řešení je možné rozšířit o specifické moduly TAP, které jsou po pořízení plně integrovatelné. Výrobce disponuje TAPy metalickými i optickými.	ANO
Integrace s monitorovaným síťovým prostředím	Nabízené řešení bude agregovat provoz z dvou DC HMP a bude jej předávat v definovaných výstupních rozhraních v libovolné lokalitě (monitorovaný provoz tak může být tunlován mezi lokalitami).	Nabízené řešení je koncipováno jako dva páry technologií (vždy jedna dvojice do každé lokality) a dokáže vstupní síťový provoz protunelovat vždy do druhé lokality.	ANO
Integrace s monitorovaným síťovým prostředím	Výstupní rozhraní budou typem média nezávislé na vstupních rozhraních monitorované sítě.	Naízené řešení slouží pro konverzi a unifikaci médií. Výstupní	ANO

		rozhraní nejsou typem a rychlosí závislé na vstupních rozhraních.	
Integrace s monitorovaným síťovým prostředím	Bude podporováno sledování provozu z virtuálního síťového přepínače virtualizační platformy VMware. Cílem je získat jednotný obraz chování sítě, včetně komunikací uvnitř virtuální platformy.	Součástí nabízeného řešení jsou licence pro pokrytí 10ti serverů pro virtualizaci pro zajištění plného vhledu do síťového provozu uvnitř hypervizorů.	ANO
Integrace s monitorovaným síťovým prostředím	Dodávané řešení bude schopno zpracovat síťový provoz o celkové kapacitě alespoň 100Gbps (údaj před optimalizací a filtrací).	Procesorový výkon nabízeného řešení pro zpracování vstupních dat je schopen pracovat se síťovým provozem až 800Gbps.	ANO
Integrace s monitorovaným síťovým prostředím	Počet vstupních rozhraní dodávaného řešení určených k integraci s monitorovanou sítí bude minimálně 20 v každém ze dvou DC HMP	Počty rozhraní pro každou lokalitu jsou: 5 x 1Gbps 20 x 10Gbps 4 x 40Gbps	ANO
Filtrování a manipulace s monitorovaným provozem	Možnost provádět filtrování síťového provozu před jeho předáním na výstupní rozhraní pro připojení analytických nástrojů. Cílem je umožnit předat jen potřebné typy komunikací pro každý připojený analytický nástroj.	Součástí nabízeného řešení je licence na filtrování obsahu provozu pro pokrytí požadované funkcionality.	ANO

Filtrování a manipulace s monitorovaným provozem	Pravidla pro filtorvání provozu musejí být definovatelná podle 4. vrstvy ISO/OSI modelu.	Filtrování dle L4 pravidel.	ANO
Filtrování a manipulace s monitorovaným provozem	Možnost provádět manipulace s provozem do monitorovacích zařízení: - Maskování citlivých informací – umožňuje bezpečnostním týmům skrýt citlivé informace a tím ochránit organizaci před porušováním nažízení plynoucích z ZoKB popř. GDPR. - Předávání jen vybrané části komunikací, které jsou předmětem zájmu připojeného monitorovacích zařízení - předávání jen hlaviček provozu bez obsahu paketů. - Doplňování dodatečných informací o zdroji monitorovaných dat pro lepší orientaci a obohacení monitoringu.	Součástí nabízeného řešení je licence na manipulaci s obsahem provozu pro pokrytí požadované funkcionality.	ANO
Filtrování a manipulace s monitorovaným provozem	Potřebné komponenty pro sledování virtuálního prostředí budou dostupné ve formátu OVA/OVF template.	Dle požadavku.	ANO
Filtrování a manipulace s monitorovaným provozem	Monitorovaný provoz u lokality jednoho DC může být v některých případech potřeba předat do výstupních rozhraní v druhém DC. Řešení tedy musí umět tunelovat provoz mezi lokalitami.	Advanced Tunneling feature je součástí nabízeného řešení.	ANO
Filtrování a manipulace s monitorovaným provozem	Monitorovaný provoz musí být v dodávaném řešení optimalizován: - Deduplikován - Odstranění nadbytečných údajů - Obohacen o metadata	De-Duplication feature je součástí nabízeného řešení.	ANO
Správa a ovládání komponnt dodávaného řešení	Možnost spravovat jednotlivé komponenty pomocí bezpečného rozhraní SSH nebo HTTPS.	Obě požadované varianty jsou podporovány.	ANO
Správa a ovládání komponnt dodávaného řešení	Možnost napojení zařízení na SIEM z důvodu monitoringu administrátorských aktivit.	Technologie loguje přístupy a logy je možné zaslat ve formátu SYSLOG na technologie 3. stran.	ANO

Správa a ovládání komponnt dodávaného řešení	Generování statistik o sledovaném síťovém provozu na všech vstupních síťových rozhraních.	Statistiky si vede každá z nabízených HW appliancí.	ANO

2.2. Bezpečnostní hraniční brány firewall pro sítě Mepnet

Bezpečnostní hraniční brány firewall pro vybraných X organizací připojených do metropolitní sítě Mepnet, jehož primárním určením je ochrana vstupního rozhraní do sítě a garance čistoty provozu. Brány budou zařazeny do současného centrálního nástroje pro správu bezpečnostní politiky MHMP a Mepnet, který je provozován na technologii Check Point.

Metropolitní síť (Mepnet), která propojuje organizace a subjekty zřízené Hlavním městem Prahou, představuje pro bezpečnost opravdovou výzvu, neboť propojuje subjekty s rozdílnou úrovní řešení vlastní bezpečnosti. Z tohoto důvodu a pro ochranu společné sítě Mepnet je požadováno dodání hraničních bran firewall, které zajistí bezpečnost vybraných přípojných míst do sítě Mepnet. Pro iniciální fázi zabezpečení bylo vybráno 5 městských organizací.

Pro jednotlivé připojené lokality je požadováno řešení, které umožní nejen ochranu přístupu do sítě mepnet, ale bude umožněno realizovat na stejném systému komplexní perimetrovou ochranu připojené lokality.

☐ **Základní údaje**	**Nabízená hodnota**
Výrobce zařízení	Check Point
Počet kusů zařízení - 5	5
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	CPAP-SG5400-NGTX
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.checkpoint.com/downloads/product-related/datasheets/ds-5400-appliance.pdf

Parametr	**Požadovaná hodnota parametru (pro jedno fyzické zařízení)**	**Nabízená hodnota (Popis)**	**Splňuje Ano/Ne**
Požadavky na HW bezpečnostní brány firewall	- Brána bude provozována na vlastním HW - Parametry pro umístění do DC: o Rozměr pro umístění v RACK do 2U o Redundantní napájení 2x230V - Zařízení bude vybaveno out-of-band management rozhraním - Rozhraní pro síťová připojení: o 8 x RJ45 10/100/1000 o Možnost rozšíření o 10GbE fiber o Podpora 802.1Q, port teaming, LACP, DHCP server/relay o Možnost řízení QoS pro jednotlivé realizované	Nabízené zařízení je dodáváno jako vlastní HW platforma (appliance) požadovaných rozměrů a s osazením dle požadovaných parametrů. Nezávislý management interface je	ANO

	komunikace (i pro šifrovaný provoz)	součástí nabízeného řešení.	
Požadavky na výkon zařízení	Propustnost systému firewall při řízení síťových komunikací: - 10 Gbps Minimální garantovaná propustnost systému při plné inspekci provozu (FW, IPS, URL filtering, IP reputation, VPN, Antivirus, Sandbox): - 350 Mbps Propustnost systému při plné inspekci provozu (FW a IPS): - 1 Gbps Propustnost provozu při šifrování AES-128 (bez inspekce): - 2 Gbps V lokalitě bude od dodaného řešení vyžadována ochrana celého perimetru s vlastní internetovou přípojkou. V lokalitě bude od dodaného řešení vyžadována ochrana intra DMZ provozu.	Všechny požadované propustnosti jsou výrobcem deklarované a nabízené řešení je splňuje bez výhrad. Přehled parametrů (real-world): FW až 10Gbps FULL 395 Mbps IPS až 1Gbps AES-128 2Gbps	ANO

Tabulka společných detailních funkčních požadavků na dodávané řešení hraničních bran firewall pro vybrané lokality:

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Centrální management síťové bezpečnosti	Dodávané řešení musí být plně kompatibilní se stávajícím nástrojem pro správu síťové bezpečnostní politiky provozovaném na platformě Check Point. Integrace musí být zajištěna na úrovni: - Správa bezpečnostní politiky - Centralizace logů z bezpečnostní brány firewall - Monitoring životních funkcí brány firewall i všech statistik o komunikacích a bezpečnostních událostech - Konfigurace síťových parametrů brány firewall - Správa licencí a subscriptions - Ovládání stavu brány firewall (aktivní, vypnutá)	Řešení je plně kompatibilní s management prostředím Check Point a nabízené brány je tak možno integrovat do současného systému správy bezpečnostní politiky.	ANO

Centrální management síťové bezpečnosti	Dodávané řešení umožní pro potřeby jednotlivých připojených lokalit definovat specifické sady bezpečnostních pravidel a umožní vlastní přístup skupiny administrátorů k této politice. Bude tak podporován tzv. více-doménový režim správy politik.	Nabízené bránové řešení je plně podrobitelné centrální správě tzv. MDM managementu, pokud tento bude provozován v prostředí MHMP.	ANO
Centrální management síťové bezpečnosti	Správa logů bude opět řešena pro jednotlivé připojené lokality zvlášť, aby nedocházelo k sdílení logů mezi správci z jednotlivých přípojných míst.	Nabízené bránové řešení je plně podrobitelné centrální správě logů v prostředí jednotného managementu MHMP.	ANO
Požadavky na bezpečnostní funkce dodané brány firewall	- Firewall - VPN (šifrování provozu site-to-site) - Intrusion Prevention System - URL filtering - Řízení provozu aplikací včetně jejich automatického rozpoznávání - Ochrana proti přístupu na známé nebezpečné cíle (např. C&C) - Sandbox ochrana před útoky typu oday Pro všechny bezpečnostní funkce bude aktivní podpora výrobce obsahující aktualizaci definic a vzorků. Jednotlivé funkcionality budou umožňovat detailní řízení pravidel pro jejich uplatnění v síťovém provozu.	Součástí nabízeného řešení je plná podpora Next Generation Threat Prevention & SandBlast a to včetně 3 roků předplatného pro definice výrobce. Podpora výrobce: Premium Collaborative Enterprise Support	ANO

2.3. Centrální kontrolér LAN sítě

Centrální kontrolér slouží jako nosič modulární platformy, která umožnuje vytvářet virtualizované prostředí nad LAN sítěmi, které umožnují automatizovaný provoz LAN aktivních prvků, které sdružuje do řízených skupin. Síťové prvky obsažené v řízené skupině se

již nekonfigurují ručně, ale přes rozhraní modulární platformy. Jednotlivé řízené skupiny můžou být geograficky oddělené avšak s IP konektivitou na centrální kontrolér.

☐ Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 3	3	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	DNA-HW-APL	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Řízení celého řešení	Centrální kontrolér	ANO
Funkce pro zcela automatické sestavení a konfiguraci fyzické infrastruktury		ANO
Veškeré síťové politiky jsou implementovány prostřednictvím centrálního kontroleru		ANO
Podpora vytváření multi-tenant prostředí - členění koncových uživatelů a zařízení do oddělených virtuálních sítí		ANO
Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jejich role, nezávisle na IP adresaci koncových zařízení a síťové topologii		ANO
Podpora funkcionality distribuované default gateway na jednotlivých edge přepínačích		ANO
Podpora mobility uživatelů a zařízení přes jednotnou infrastrukturou bez nutnosti vytvářet L2 broadcast domény		ANO
Integrace WLAN infrastruktury s možností terminovat datový provoz od bezdrátově připojených uživatelů přímo na edge přepínačích		ANO
Společné politiky pro pevně i bezdrátově připojené uživatele		ANO
Centralizovaná definice pravidel pro řízení přístupu uživatelů a zařízení v síti		ANO
Podpora real time telemetrie, schopnost monitorovat každý paket, každý datový tok procházející infrastrukturou		ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Požadovaná funkcionalita centrálního kontroleru		
Formát zařízení	HW appliance	ANO
Typ zařízení	SDN kontroler	ANO
Redundantní nasazení		ANO
Grafické uživatelské rozhraní součástí řešení		ANO

Přístupová práva založená na uživatelských rolích		ANO
Otevřené API rozhraní pro integraci s externími systémy		ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí kontroleru		ANO
Pokročilá správa operačního systému síťových zařízení ☐ Patching management ☐ SW Image Rollback ☐ Verifikace integrity SW image		ANO
Inventarizace nasazeného HW		ANO
Hierarchické zobrazení topologické mapy včetně jejího členění na jednotlivé lokality		ANO
GUI rozhraní pro detailní přehled o výkonnosti a stavu celé komunikační infrastruktury včetně monitorování stavu jednotlivých zařízení (využití CPU, DRAM paměti, jednotlivých síťových rozhraní atd.)		ANO
Konfigurace sítě a síťových politik prostřednictvím předefinovaných workflows		ANO
Podpora mikrosegmentace - členění koncových uživatelů a zařízení do logických skupin podle jeho identity. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky (bezpečnostní politiky) vůči jiným skupinám		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO

Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.4. Monitorování datových toků

Nástroj pro monitorování sítě s primárním zaměřením na identifikaci bezpečnostních incidentů. S použitím NetFlow a Advanced Security analyzuje i šifrovanou komunikaci a dokáže porovnat síťový provoz proti databázi bezpečnostních hrozeb udržovanou výrobcem. Obraný perimetr se tak posunuje na síťovou vrstvu, kde je umožněno zachytávat hrozby i pro antivirovými programy nevybavené zařízení jakou jsou IP Telefony, CCTV kamery apod. Používá NetFlow záznamy shromážděné z exportu od všech připojených zařízeních v síti. Systém shromažďuje informace Netflow, IPFIX, sFlow, stejně jako ekvivalenty třetích stran (jFlow). Korelace těchto informací společně umožnuje nahlédnout na zdrojovou a cílovou adresu, zdrojový a cílový port, rozhraní, IP TOS, IP protokol, Next Hop IP, TCP značky, stejně jako na informace L7 aplikací pomocí flowsensorů.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet setů zařízení: Management 1ks, Collector 1ks, UDP replikátor 2ks	4ks celkem	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	ST-SMC2200-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com /c/en/us /products/security /stealthwatch /index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Formát zařízení	HW appliance	ANO
Centrální správa appliancí (kolektorů, senzorů, atd.) pro sběr a analýzu dat, případně dalších komponent systému, distribuovaných v síti		ANO
Možnost sběru dat/integrace s dalšími bezpečnostními prvky a systémy (firewall, web proxy, IDS/IPS, systémy řízení přístupu do sítě, ...)		ANO
Sběr dat a jejich prezentace z velkého množství rozdílných síťových segmentů současně (z distribuovaných appliancí)		ANO
Vizibilita napříč pevným i virtuálním prostředím		ANO

Detekce a prioritizace bezpečnostních hrozeb		ANO
Detekce porušení požadovaných politik		ANO
Dostatečně 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
Různé skupiny oznámení (alarmů)		ANO
Přehledové zobrazení všech oznámení (alarmů) na hlavní monitorovací obrazovce		ANO
Seskupování a grafická reprezentace vztahů a toků mezi logickými skupinami (definovanými uživatelem) komunikační infrastruktury		ANO
Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu		ANO
Napojení na centrální databázi hrozeb poskytovanou výrobcem, která je neustále aktualizovaná		ANO
Integrace se systémem řízení přístupu do sítě pro provádění automatizovaných nápravných akcí		ANO
Integrace se SIEM systémy, minimálně ArcSight a Splunk		ANO
Funkcionality dostupné i pomocí REST API		ANO
Implementace rozhraní pro sdílení informací s jinými bezpečnostními systémy - pxGrid nebo draft-ietf-mile-xmpp-grid-02		ANO
Přístup administrátorů/uživatelů k systému podle uživatelských rolí/přístupových práv		ANO
Appliance pro analýzu a kolektování dat z transportních zařízení		ANO
Sběr dat o datových tocích ze síťových zařízení		ANO
Baselining běžného provozu		ANO
Detekce anomálií oproti běžnému provozu i na L7		ANO
Detekce anomálií na základě toků v síti		ANO
Deduplikace záznamů o toku, pokud byl tentýž tok sebrán z více zařízení v síti		ANO
Spojení všech záznamů o toku, pokud se týkají té samé transakce mezi koncovými zařízeními, včetně zařízení z veřejného Internetu		ANO
Historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu		ANO
Schopnost obohatit záznam toků o URL nebo uživatelskou aplikaci		ANO
Detekce úniku dat z organizace (Data Hoarding, Data Exfiltration)		ANO
Detekce šíření Malware		ANO
Detekce Botnetů		ANO
Detekce DDoS		ANO
Detekce scanu sítě		ANO
Min. počet spravovaných appliancí pro sběr a analýzu dat distribuovaných v síti	25	ANO

Min. kapacita databáze pro historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	2 TB	ANO
Minimální počet zpracovaných toků za vteřinu (FPS, Flows per second)	120000	ANO
Minimální počet síťových zařízení exportujících do jedné appliance pro sběr dat	2000	2000
Minimální kapacita databáze pro historický záznam všech síťových spojení pro pozdější audit a forenzní analýzu	4 TB	ANO
Možnost sbírat a analyzovat agregovaně FPS (flow per second)	6 mil. FPS	ANO
Licence pro monitorování FPS (flow per second)	15000 FPS	ANO
Licence pro monitorování koncových bodů po minimálně dobu 5 let	5300	ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.5. Řízení přístupu k síťovým prostředkům (802.1x)

Řešení integruje funkcionalitu univerzálního autentizačního a autorizačního systému s jednotnou správou. Produkt je zaměřený na zjištění a prověření stavu koncových stanic, které se přihlašují do sítě (LAN, W-LAN, VPN). Centralizované řešení pro kontrolu přístupu do sítě dokáže ověřit, zda stanice, které se připojují do sítě, vyhovují bezpečnostním pravidlům stanoveným v organizaci.

Univerzální integrační platforma je rozhraní s otevřenou podporou více výrobců, síťových prvků nebo systémů. Umožňuje spolupráci mezi různými platformami IT infrastruktury, jako

jsou platformy pro monitorování bezpečnosti, detekční systémy, platformy na definici síťových bezpečnostních politik, správu zařízení a konfigurace, správu přístupu do sítě a identity uživatele.

☐ Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 4	4	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	SW-3595-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com /c/en/us/products/ Security/identity-services-engine/index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Obecná charakteristika ověřovacího řešení		ANO
Centralizovaný systém pro ověřování uživatelů, nebo koncových zařízení, 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 apod.)	5300	ANO
Formát zařízení	HW appliance	ANO
CPU	8 vCPU	ANO
Paměť	64GB	ANO
Disková kapacita	2,4 TB, RAID 10	ANO
Disková propustnost (I/O Speed)	300 MBps	ANO
počet připojených koncových uživatelů	20000	ANO
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
V rámci ekosystému vytvořenému pomocí integrační platformy musí být možno použít adaptivní řízení síťových prvků organizace, které umožnuje rychle reagovat na útoky metodou přímého využití sítě jako vynucovacího prostředku (konkrétní scénáře odpojení uživatele). V praxi toto může znamenat odpojení problematického koncového zařízení přímo od rozhraní LAN přepínače nebo od WiFi přístupového prvku na základě signalizace od detekčního bezpečnostního systému umístěného uvnitř sítě.		ANO
Integrace s NGFW, kde nástroj pro kontrolu přístupu do sítě na základě sdílených informací může infikované koncové zařízení pozorovat, omezit jim přístup, nebo napomoci v remediačním procesu		ANO
Poskytuje AAA funkce (viz níže)		ANO
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)		ANO
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity		ANO

Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace		ANO
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)		ANO
Je dostupné ve formě Virtuálního stroje na platformách ESX nebo ESXi		ANO
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		ANO
Podporované protokoly		ANO
RADIUS pro autentizaci, autorizaci a accounting		ANO
proxy funkce pro externí RADIUS		ANO
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST, EAP-FAST s podporou EAP-Chaining		ANO
Podporované databáze uživatelů (s možností definovat pořadí autentizace		ANO
Interní (pro uživatele i koncová zařízení)		ANO
Active Directory		ANO
Active Directory – více nezávislých domén		ANO
LDAP (RFC 2251)		ANO
RADIUS Token indentity source (RFC 2865)		ANO
RSA RADIUS token server		ANO
Autentizace pomocí údajů obsažených v uživatelském certifikátu		ANO
Ověřování uživatelů a zařízení		ANO
Ověření uživatelů heslem nebo certifikátem		ANO
Ověření MAC adresou připojovaného zařízení		ANO
Rozpoznávání typu koncových zařízení a jejich stavu		ANO
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou		ANO
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbianOS, Apple, Blackberry, HTC)		ANO
Ověření stavu koncových zařízení pomocí softwarového agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat		ANO
☐☐instalovaný operační systém (Windows 7/10)		ANO
☐☐opravy instalované v operačním systému		ANO
☐ verze instalovaných programů		ANO
☐☐hodnoty položek v registry databázi systémů Windows		ANO
☐☐stav aplikací, zejména antivirů		ANO
Autorizace: flexibilní systém pro definici pravidel pro přístup k síti		ANO
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle		ANO
☐☐uživatele (role, skupiny),		ANO
☐☐stavu a typu koncového zařízení (viz výše),		ANO

□□místa připojení,		ANO
□□historie připojení		ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě		ANO
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě		ANO
Podpora Change of Authorization (CoA, RFC 3576)		ANO
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti		ANO
Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem, spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru)		ANO
Accounting		ANO
Zaznamenávání aktivity uživatelů a zařízení připojených k síti		ANO
Dotazovací systém, korelace záznamů, centralizované výkazy		ANO
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)		ANO
Funkce GUEST serveru		ANO
Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi		ANO
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů		ANO
Samoobslužný portál pro uživatele		ANO
Ověření přes HTTP a HTTPS		ANO
Rozhraní pro integraci s externími operátory pro zasílání SMS zpráv s autentizačními údaji		ANO
Další vlastnosti		ANO
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)		ANO
Integrace s MDM systémy		ANO
Možnost vyčítání informací o uživateli z Active Directory (Passive Fingerprint)		ANO
Funkce pro správu ověřovacího systému		ANO
Centralizovaná správa		ANO
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému		ANO
Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení		ANO
Grafické rozhraní pro definici pravidel přístupu k síti		ANO
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů		ANO
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)		ANO
Zaznamenávání událostí na externí syslog server		ANO
NTP pro synchronizaci času		ANO
SMTP pro zasílání zpráv a výstrah přes e-mail		ANO

Řízení přístupu na síťová zařízení		
Podpora protokolu TACACS+ pro možnost řízení přístupu administrátorů na síťová zařízení		ANO
Proxy TACACS+		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.6. Správa síťového prostředí

Komplexní řešení pro správu, vizualizaci a monitorování sítě z jednoho grafického rozhraní. Řešení zajišťuje viditelnost sítí a aplikací, zálohy konfigurací, zjednodušení nasazení a správy zařízení.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 1	1ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	PI-UCS-APL-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com /c/en/us /products/cloud-systems-management/prime-infrastructure/index.html	
Požadovaná hodnota parametru	**Minimální Požadavky**	**Splněno (ANO/NE)**
Dostupné v provedení připraveného virtuálního stroje do virtualizovaného prostředí		ANO

Dostupné v provedení fyzické appliance (samostatné zařízení)		ANO
Formát zařízení	HW appliance	ANO
CPU	10 vCPU	ANO
Paměť	64 GB	ANO
Disková kapacita SSD	3,6 TB, RAID 10	ANO
Disková propustnost (I/O Speed)	550 MBps	ANO
Událostí zpracovaných za jednu sekundu celkem	930	ANO
Syslog zpráv zpracovaných za jednu sekundu	550	ANO
SNMP trapů zpracovaných za jednu sekundu	280	ANO
Systémových událostí zpracovaných za jednu sekundu	80	ANO
Zpracovaných toků Netflow - Netflow flow za sekundu	70000	ANO
Volitelné navýšení počtu zpracovaných toků Netflow - Netflow flow za sekundu	300	ANO
Podpora funkcí pro kontrolu konfigurací na souladu s doporučenými konfiguracemi (best practices)		ANO
Podpora funkcí pro kontrolu přítomnosti známých bezpečnostních chyb v nahrazeném SW spravované síťové infrastruktury		ANO
Podpora funkcí pro kontrolu milníků HW a SW spravované síťové infrastruktury - zajištění zdraví sítě (konec podpory HW, SW apod.)		ANO
Platforma		ANO
Bezpečný přístup prostřednictvím webového grafického uživatelského rozhraní		ANO
Podpora autorizace a autentizace přístupu do systému vůči TACACS+		ANO
Podpora autorizace a autentizace přístupu do systému vůči RADIUS		ANO
Podpora řízení přístupu ke GUI pomocí identity (SSO - Single Sign On)		ANO
Podpora různých úrovní oprávnění pro přístup do systému (RBAC)		ANO
Podpora multi - uživatelského prostředí GUI s možností využít jak předdefinované skupiny, tak s možností definovat vlastní přístupová oprávnění k funkcím GUI pro alespoň dvě uživatelské skupiny		ANO
Podpora přístupu ke GUI z mobilních zařízení, např. tabletů		ANO
Podpora logování aktivity uživatelů a logování systémových událostí		ANO
Podpora zálohování systému a obnovy ze zálohy		ANO
Možnost redundance pro zajištění vysoké dostupnosti, automatická synchronizace		ANO
Možnost změnit nastavení doby ukládání historických a agregovaných dat		ANO
Možnost omezit přístup uživatelům pouze ke skupině zařízení, např. na základě lokality, typů zařízení apod.		ANO
Možnost monitoringu provozních parametrů aplikací		ANO

Možnost zpracování informací o provozu v síti (NetFlow) včetně deduplikace dat z více zdrojů		ANO
Možnost zobrazit informace o chování aplikací v síti (statistiky, identifikace případných problémů na síťové nebo aplikační úrovni, zhoršení uživatelské zkušenosti uživatelů)		ANO
Podpora protokolu IPv4		ANO
Podpora protokolu IPv6		ANO
Podpora protokolu SSH		ANO
Podpora protokolů SNMPv1, SNMPv2, SNMPv2c a SNMPv3		ANO
Podpora zpracování SYSLOG zpráv		ANO
Podpora zpracování SNMP zpráv		ANO
Možnost úpravy zpracování událostí a alarmů včetně např. potlačení vybraných alarmů		ANO
Možnost kategorizace alarmů a událostí		ANO
Možnost nastavit zasílání upozornění na vybrané události emailem		ANO
Podpora MIB třetích stran		ANO
Možnost monitoringu parametrů definovaných v MIB třetích stran		ANO
Možnost definovat vlastní události na základě SNMP nebo SYSLOG zpráv		ANO
Možnost exportu zpráva a událostí		ANO
Možnost generovat zprávy pro nadřazený management systém		ANO
Posílání alarmů a událostí network management aplikacím třetích stran, které podporují FCAPS		ANO
Podpora API pro programatický přístup k funkcionalitě aplikace správy		ANO
Schopnost management systému nalézt automaticky zařízení v síti s využitím více různých metod pracujících s informacemi z druhé a třetí vrstvy		ANO
Schopnost management systému filtrovat nalezená zařízení – vyloučit resp. zahrnout definované adresní rozsahy		ANO
Schopnost management systému připravit konfigurační a jiné změny formou úlohy včetně schvalovacích mechanizmů		ANO
Podpora pro vyhledávání informací o síťových zařízení, připojených koncových zařízení, uživatelích, konfigurovaných parametrech, alaremech, událostech apod. napříč celým management systémem.		ANO
Správa aktivních prvků		ANO
Požadovaný počet spravovaných aktivních prvků	215	ANO
Požadavky na škálování - minimální počet spravovaných zařízení LAN / WAN sítě - aktivních prvků	2000	ANO
Požadavky na škálování - systém musí být schopen kromě LAN / WAN sítě spravovat a monitorovat také bezdrátovou síť pouhým přidáním příslušných licencí		ANO
Kompletní správa životního cyklu LAN / WAN sítě (plánování, nasazení, monitoring, troubleshooting, reporting)		ANO
Inventarizace HW síťových prvků		ANO

Inventarizace, nasazení a správa firmware aktivních prvků		ANO
Analýza vhodnosti firmware aktivních prvků pro nasazení		ANO
Generování reportů inventory aktivních prvků		ANO
Konfigurace pomocí šablon pro zefektivnění konfiguračních úloh		ANO
Inventarizace, verzování, archivace a správa konfigurací LAN/WAN sítě		ANO
Předpřipravené šablony dle doporučení výrobce - "best practice"		ANO
Možnost udržovat konfigurace v souladu s firemním standardem, identifikovat neshody		ANO
Možnost vytvářet vlastní konfigurační šablony (sekvence příkazů)		ANO
Celkové konfigurační šablony sestavovány z dílčích šablon konfigurací jednotlivých funkcí nebo uživatelsky definovaných konfigurací jednotlivých funkcí		ANO
Podpora pro o automatizovanou konfiguraci nově připojovaných zařízení		ANO
Zobrazování alarmů a událostí z LAN / WAN sítě		ANO
Topologická mapa		ANO
Nástroje pro detekci a řešení problémů v LAN / WAN síti		ANO
Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souhrnném pohledu (kontextově) pro rychlejší troubleshooting		ANO
Zobrazení informací o uživateli, koncovém či síťovém zařízení v kontextu informací souvisejících s jeho okolím a provozními parametry		ANO
Detailní monitoring LAN / WAN sítě		ANO
Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí		ANO
Monitorování výskytu koncových zařízení a uživatelů v síti		ANO
Monitoring a vyhodnocování přenosových parametrů z NetFlow		ANO
Monitoring funkčnosti (včetně odezev) přenášených aplikací		ANO
Monitoring parametrů zdraví aktivních prvků a jejich přehledné zobrazení		ANO
Možnost nastavit prahové hodnoty pro monitoring parametrů zdraví aktivních prvků		ANO
Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí		ANO
Automatické dohledání portu pevné sítě s připojeným falešným access pointem		ANO
Možnost identifikovaný problém eskalovat prostředky management systému na podporu výrobce		ANO
Integrace s další aplikací pro zjišťování identity, typu, parametrů, stavu a stavu software koncových klientů pevné i bezdrátové sítě; pro monitoring bezpečnostních politik koncových klientů (ISE server)		ANO
Správa serverů a virtuálních appliace – volitelně		ANO
Možnost rozšíření o správu a monitoring připojených Cisco UCS serverů		ANO

Možnost rozšíření o správu a monitoring virtuálních strojů běžících na ESXi host (spolupráce s vCenter)		ANO
Možnost rozšíření o zpracování událostí souvisejících s výpadkem konektivity nebo chybou komponenty Cisco UCS serveru		ANO
Možnost rozšíření o schopnost detekovat výpadek Cisco UCS blade serveru, identifikovat správný blade server a graficky zobrazit vazby		ANO
Možnost rozšíření o zobrazení vazby mezi monitorovaným virtuálním strojem na ESXi hostu běžícím na Cisco UCS serveru a tímto serverem		ANO
Možnost rozšíření o sledování výkonnostních parametrů monitorovaných Cisco UCS serverů		ANO
Možnost rozšíření o sledování výkonnostních parametrů monitorovaných virtuálních strojů		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.7. Datacentrové řešení Spine-Leaf

Centralizovaná správa a konfigurace komunikační infrastruktury datového centra prostřednictvím grafického uživatelského rozhraní nebo s využitím externích nástrojů využívajících otevřená aplikační rozhraní (např. REST API). Integrovaná a centralizovaná správa jak fyzické, tak virtuální síťové infrastruktury datového centra prostřednictvím kontroléru. Definice aplikačních politik s využitím objektově orientovaných datových modelů místo používání tradičních síťových struktur (VLAN, ACL, IP subnet..). Plně automatizovaná konfigurace komunikačních prvků a systémů datového centra na základě definovaných aplikačních politik a s využitím otevřených aplikačních rozhraní (např. OpFlex)

Základní údaje	Nabízená hodnota	
Výrobce zařízení	CISCO	
Technologický celek - 1 fabrika	1 fabrika	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	APIC-SLUSTER-L2	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Formát zařízení	HW appliance	ANO
Architektura řešení – **„Spine – Leaf“**		ANO
Řízení celého řešení „DC Fabric“ prostřednictvím řadiče (kontroleru)		ANO
OSPFv2		ANO
OSPFv3		ANO
IS-IS		ANO
BGPv4		ANO
BGPv6		ANO
802.1q		ANO
VXLAN enkapsulace		ANO
VXLAN bridging		ANO
VXLAN routing		ANO
Integrace fyzických i virtuálních zařízení pro L4-L7 služby		ANO
☐☐Integrace s Hypervisorem VMware vSphere		ANO
☐ Integrace s Hypervisorem Microsoft Hyper-V		ANO
☐ Integrace se zařízením F5		ANO
☐ Integrace se zařízením Cisco ASA		ANO
Congestion-aware load balancing datového provozu		ANO
Podpora vytváření multi-tenant prostředí		ANO
Požadovaná funkcionalita centrálního řadiče (controlleru)		
Řadič s redundancí pro každé datové centrum		ANO
Mód činnosti řadičů – všechny aktivní		ANO
Grafické uživatelské rozhraní součástí řešení		ANO
Přístupová práva založená na uživatelských rolích		ANO
Možnost rozdělit správu řešení mezi více vzájemně oddělených organizací (multitenantní řešení)		ANO
Dokumentované API rozhraní pro volání všech dostupných funkcí řadiče, včetně těch, které jsou použity v grafickém uživatelském rozhraní		ANO

Možnost řízení aplikačních toků prostřednictvím definice aplikačních politik, které formou logického modelu popisují požadavky aplikací na síťovou konektivitu, bezpečnost a L4-L7 služby		ANO
Možnost členění fyzických a virtuálních serverů do logických skupin podle své funkce a na základě charakteristik, jako je IP adresa, MAC adresa, příslušnosti do VLAN, VXLAN. Ke skupinám jsou pak definovány na abstraktní úrovni komunikační požadavky vůči jiným skupinám.		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.8. Spine vrstva

Základní údaje	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 2	2ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	N9K-C9364C	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-731792.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ přepínače	L2/L3 přepínač	ANO

Formát zařízení	fixní	ANO
Redundantní zdroj		ANO
Celková propustnost přepínače	2,88Tbps	ANO
Počet neblokovaných portů 40GE s volitelným fyzickým rozhraním typu QSFP+	36	ANO
Podpora QSFP+ rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN enkapsulace		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
Podpora LAG, možnost konfigurace až **32** linek v rámci jednoho LAG		ANO
Počet konfigurovatelných LAGs	256	ANO
Podpora "jumbo rámců"	9216 bytů	ANO
IEEE 802.1Q		ANO
Počet aktivních VLAN	4000	ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Počet MAC záznamů	80000	ANO
Počet host IPv4 routes	200000	ANO
Počet host IPv6 routes	40000	ANO
OSPFv2		ANO
IS-IS		ANO
BGP		ANO
ECMP	64 cest	ANO
Virtualizace směrovacích tabulek (např. Virtual Routing and Forwarding (VRF)	500	ANO
OSPFv3		ANO
MP BGP		ANO
QoS – Priority Based Flow Control (IEEE 802.1Qbb)		ANO
WRED		ANO
Funkce ochrany přepínače před útoky typu odepření služby (DoS) formou vhodného omezení frekvence určitých typů rámců/paketů, které jsou zpracovávány procesorem zařízení (např. Control Plane Policing nebo ekvivalentní funkcionalita)		ANO
OpenStack Neutron Plug-in		ANO
Python scripting		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO

Vzdálený port mirroring		ANO
Syslog		ANO
Distribuovaná správa přístupů na základě rolí (Role Based Access Control)		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.9. Leaf vrstva – 10GB SFP+

Základní údaje	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 4	4ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C1-N9K-C93180YC-FX	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com /c/en/us /products/switches /nexus-93180yc-fx-switch/index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ přepínače	L2/L3 přepínač	ANO
Formát zařízení	fixní	ANO
Redundantní zdroj		ANO
Celková propustnost přepínače	3,6 Tbps	ANO

Počet neblokovaných portů typu 10/25GE s volitelným fyzickým rozhraním	48	ANO
Počet neblokovaných portů 40/100GE s volitelným fyzickým rozhraním typu QSFP+	6	ANO
Podpora QSFP rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN bridging		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3900	ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	96000	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS – Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Droping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Možnost rozšířit funkcionalitu přepínače o podporu technologie FC/FCoE NPV na SFP portech, např. formou licence		ANO
HW podpora IEEE 802.1ae (AES-GCM-XPN-256) na všech SFP a QSFP portech		ANO
Minimální počet host IPv4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO
BGP/MP-BGP		ANO
ECMP	64 cest	ANO
IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM BiDir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
First Hop Redundancy Protokol pro IPv6		ANO

Port ACL, VLAN ACL		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence		ANO
Integrovaná Flow table	32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetrie pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.) - gRPC/GPB transport		ANO
Streaming telemetrie - time-based a event-based triggers		ANO
Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autoprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO
Syslog		ANO
Role Based Access Control		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO

V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.10. Leaf vrstva 10GB – RJ45

Základní údaje	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 2	2ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C1-N9K-C93108TC-FX	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736651.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ přepínače	L2/L3 přepínač	ANO
Formát zařízení	Fixní	ANO
Redundantní AC zdroj (front-to-back airflow)		ANO
Celková propustnost přepínače	2,16 Tbps	ANO
Minimální počet neblokovaných portů typu typu 1/10GBASE-T	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	6	ANO
Podpora 40GE rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3900	ANO

Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	96000	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS – Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Droping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
HW podpora IEEE 802.1ae (AES-GCM-XPN-256)		ANO
Minimální počet host IPv4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO
BGP/MP-BGP		ANO
ECMP	64 cest	ANO
IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM BiDir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
First Hop Redundancy Protokol pro IPv6		ANO
Port ACL, VLAN ACL		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence		ANO
Integrovaná Flow table	32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetrie pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.) - gRPC/GPB transport		ANO
Streaming telemetrie - time-based a event-based triggers		ANO

Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autoprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO
Syslog		ANO
Role Based Access Control		ANO
Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.11. Leaf vrstva 1GB – RJ45

Základní údaje	**Nabízená hodnota**
Výrobce zařízení	CISCO
Počet kusů zařízení - 10	10ks
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	N9K-C9348GC-FXP

Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com /c/en/us/products /collateral/switches/nexus-9000-series-switches/datasheet-c78-738259.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ přepínače	L2/L3 přepínač	ANO
Formát zařízení	Fixní	ANO
Redundantní AC zdroj (front-to-back airflow)		ANO
Celková propustnost přepínače	690Gbps	ANO
Minimální počet portů 100/1000Base-T	48	ANO
Minimální počet neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28	2	ANO
Minimální počet portů 10/25GE s volitelným fyzickým rozhraním typu SFP	4	ANO
Podpora 40GE rozhraní umožňujících přenos signálu přes duplexní multimodová vlákna typu OM3, resp. OM4		ANO
VXLAN routing		ANO
VXLAN with MP-BGP EVPN control plane		ANO
IEEE 802.3ad		ANO
IEEE 802.3ad přes více šasi (Multichassis Link Aggregation)		ANO
Minimálně 32 linek jako součást Link Aggregation Group		ANO
Minimální počet konfigurovatelných Link Aggregation Groups	256	ANO
Podpora "jumbo rámců"	9216 bytes	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	3900	ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Detekce protilehlého zařízení (např. LLDP)		ANO
Minimální počet MAC záznamů	96000	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS – Priority Based Flow Control (IEEE 802.1Qbb)		ANO
Approximate Fair Droping		ANO
Možnost zobrazit využití bufferů per port a per queue v reálném čase		ANO
Min. velikost sdíleného systémového bufferu	40MB	ANO
Minimální počet host IPv4 routes	100000	ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
OSPFv2/OSPFv3		ANO
BGP/MP-BGP		ANO
ECMP	64 cest	ANO

IGMPv2, IGMPv3		ANO
MLDv2		ANO
IGMP snooping		ANO
IP Multicast (PIM SM, PIM SSM) pro IPv4 i IPv6		ANO
PIM BiDir		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
First Hop Redundancy Protokol pro IPv6		ANO
Port ACL, VLAN ACL		ANO
IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping)		ANO
Možnost rozšířit funkcionalitu přepínače o podporu line rate flow telemetrie (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence		ANO
Integrovaná Flow table	32000 záznamů	ANO
Možnost exportovat monitorovaná data ve formátu NetFlow v9 nebo IPFIX		ANO
Control Plane Policing		ANO
Integrace s VMware vCenter umožňující zobrazit virtuální servery připojené na jednotlivé fyzické porty přepínače		ANO
Integrace s VMware vCenter umožňující automatickou konfiguraci VLAN instancí pro připojení virtuálních serverů		ANO
Programovatelnost prostřednictvím rozhraní NETCONF/YANG		ANO
Streaming telemetrie pro real-time streaming stavových a statistických informací (interface counters, interface status, BGP neighbor state, VLANs apod.) - gRPC/GPB transport		ANO
Streaming telemetrie - time-based a event-based triggers		ANO
Python scripting		ANO
Puppet, Chef programming		ANO
Power-on autoprovisioning		ANO
CLI rozhraní		ANO
SSHv2		ANO
SNMPv3		ANO
NTP server		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Port mirroring (SPAN)		ANO
Vzdálený port mirroring		ANO
Počet SPAN spojení	4	ANO
Syslog		ANO
Role Based Access Control		ANO

Součástí ceny zařízení musí být úkony záručního servisu a právo užívání software, které lze zahrnout do standardů záruky za jakost běžně užívaných v tomto segmentu trhu pro dané plnění – tj. uchazeč je povinen při dodávce zboží řádným způsobem uzavřít záruční dohodu o podpoře s výrobcem zařízení tak, aby v případě závady v průběhu celé pětileté záruky na dodaných zařízeních, kterou není Uchazeč schopen sám odstranit, bylo možné v režime 8x5xNBD tuto závadu eskalovat přímo k technické podpoře výrobce zařízení. Zadavatel musí mít možnost v průběhu pětileté záruky si sám či automaticky legálně stahovat nové verze software a operačního systému poptávaných zařízení přímo ze stránek výrobce na základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		ANO
V databázi výrobce musí být Zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Uchazeč je povinen doložit potvrzení od výrobce o určení dodávaného HW a SW pro evropský trh a Zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.		ANO
Součástí nabídky musí být doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce tohoto řešení má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.		ANO

2.12. Next-Generation Firewall

Základní údaje	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 2ks	2ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	FPR4120-ASA-K9	
Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce	https://www.cisco.com/c/en/us/support/security/firepower-4120-security-appliance/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ zařízení	Firewall	ANO
Formát zařízení	1RU	ANO
Minimální počet 1G/10G (SFP+) Ethernet portů pro management, standardně osazených	1	ANO
Minimální počet 1G/10G (SFP+) Ethernet portů pro data, standardně osazených	8	ANO
Podporovaný počet současně otevřených spojení přes FW	15 mil	ANO

Rychlost vytváření nových spojení přes FW	250 000/s	ANO
Propustnost firewallu	50 Gbps	ANO
Propustnost firewallu (multiprotokolový režim)	25 Gbps	ANO
Podpora L2 (transparentního) módu s podporou NAT a PAT		ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT		ANO
Podpora současně L2 a L3 v různých virtuálních FW		ANO
Podporovaný počet VLAN	1024	ANO
Redundance jednotlivých komponent v navrhované síti (fail-over bez přerušení spojení)		ANO
Podpora stateful failover - active/active i active/standby		ANO
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru		ANO
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP		ANO
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru		ANO
Možnost sloučení až osmi fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP		ANO
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů, přikoupením licence v případě potřeby		ANO
Dynamické směrování - podpora alespoň EIGRP (RFC7868)		ANO
OSPF, BGP		ANO
Podpora IPv6 dynamického směrování – alespoň OSPFv3		ANO
Podpora Policy based Routing		ANO
Podpora samostatných směrovacích instancí na úrovni virtuálních kontextů		ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky,jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.		ANO
Podpora filtrace IPv4, IPv6		ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD		ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích		ANO
Stateful inspekce minimálně těchto aplikačních protokolů: HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMPT, DNS, RPC, CIFS, MSRPC, NETBIOS		ANO
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu		ANO
Podpora NAT64 a DNS64		ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně		ANO

pro řízení přístupu podle uživatelské identity, typu aplikace, apod.		
Možnost rozšíření o funkce NextGen FW		ANO
Možnost rozšíření o funkce NextGen IPS		ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele		ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy		ANO
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)		ANO
Možnost správy fw pravidel přes příkazový řádek z lokální konzole a vzdáleným přístupem protokolem ssh		ANO
Vzdálené správa konfigurace přes grafické rozhraní bez nutnosti instalace tlustého klienta+A28		ANO
Při použití clusteru se spravuje pouze jeden logický prvek		ANO
Distribuce a správa SW firewallu, dalších modulů (např. pro VPN), konfigurací, licencí z grafického rozhraní managementu		ANO
Zobrazení logů a událostí v grafickém rozhraní správy s mapováním na konfiguraci bezpečnostních politik		ANO
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování		ANO
Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap		ANO
Výkon a funkcionalita VPN (požadováno)		
Propoustnost VPN koncentrátoru (šifrování 3DES/AES)	10Gbps	ANO
Počet současných šifrovaných spojení	10000	ANO
Podpora IPSec VPN		ANO
IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol		ANO
Podpora nového protokolu pro výměny klíčů IKEv2		ANO
Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256		ANO
Podpora kontrolních mechanizmů: MD5, SHA		ANO
Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256		ANO
Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384		ANO
Podpora šifrovacích algoritmů eliptických křivek (součást Suite-B): ECDH, ECDSA		ANO
Podpora SSL VPN		ANO
Jednotný klient pro IPsec (IKEv2) i SSL VPN		ANO
SSL VPN klient k dispozici pro všechny běžné desktopové OS: XP SP2+ 32-bit(x86) a 64-bit(x64), Vista (32-bit a 64-bit), Windows 7 (32-bit a 64-bit), MAC OS X(10.5, 10.6.x, 10.7.x, 10.8.x), Linux		ANO

VPN klient může být distribuovaný s 802.1X modulem řešící i efektivní machine/user autentizaci podle EAP-FAST (EAP Chaining)		ANO
VPN klient má vlastní modul pro diagnózu a reporting pro řešení případných problémů		ANO
SSL VPN klient je k dispozici pro moderní mobilní platformy na bázi Android a Apple iOS.		ANO
Podpora TLS i DTLS pro SSL připojení		ANO
Podpora SSL VPN v tunelovém režimu s distribucí VPN klientského SW přímo z FW		ANO
Podpora současné autentizace koncové stanice i uživatele		ANO
Podpora definice pravidel pro VPN přístup přímo prostředky FW		ANO
Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů		ANO
Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)		ANO
Podpora definice různých LDAP nebo AD serverů podle mapování uživatelů na skupiny s využitím RADIUS, LDAP nebo hodnot v certifikátu		ANO
Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačních systému		ANO
Podpora autentizačních mechanizmů: lokální databáze na FW, RADIUS, Windows NT LAN Manager (NTLM), Active Directory Kerberos, RSA softID, RSA securID, Lightweight Directory Access Protocol (LDAP), digitální certifikáty (X.509), smartcards		ANO
Podpora veřejných CA, včetně možnosti CA přímo na firewallu		ANO
Možnost současné autentizace AAA a certifikátem		ANO
Možnost mapování některého DN pole certifikátu na uživatelskou identitu		ANO
Podpora CRL a OCSP pro kontrolu revokace certifikátu		ANO
Podpora čistého IPv6 přístupu na VPN koncentrátor		ANO
Funkce IPS (v případě rozšíření)		
Propustnost aplikačního FW (next-gen FW) – (top parametry)	20Gbps	ANO
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	15Gbps	ANO
Propustnost aplikačního FW nebo IPS (next-gen FW, IPS) (transakční profil, 440B HTTP průměrná velikost paketu)	8Gbps	ANO
Možnost definovat typ provozu předávaný k inspekci do IPS		ANO
Podpora také IDS režimu – pasivního monitorování (TAP režim)		ANO
Možnost definovat bypass provozu při zahlcení nebo nedostupnosti IPS funkcí		ANO
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti		ANO

Podpora 802.1Q tagovaných rámců		ANO
Inspekce pro IPv4 i IPv6		ANO
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému		ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií		ANO
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací		ANO
Podpora aplikace pro psaní zákaznických filtrů		ANO
Podpora importu komunitních filtrů/signatur Snort		ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit		ANO
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS		ANO
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host" jako je spyware, phishing nebo Botnet C&C		ANO
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii		ANO
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události		ANO
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku		ANO
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive		ANO
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí		ANO
Možnost definice uživatelské vrstvy politik		ANO
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik		ANO
Různé politiky lze sdílet a aplikovat na různé senzory		ANO
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů		ANO
Ochrana před malware typu „zero day attack" které nelze detekovat tradičními antiviry		ANO
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat		ANO
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole		ANO
Možnost ochrany před malware až do úrovně koncových		ANO

stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun		
malware do karantény, blacklistů pro síťovou komunikaci, apod.		ANO
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény		ANO
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice		ANO
IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků		ANO
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“		ANO
Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.		ANO
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.		ANO
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly		ANO
Podpora databází reputací adres v Internetu (Security Intelligence)		ANO
Funkce Next-Gen FW (v případě rozšíření)		
Možnost definovat typ provozu předávaný k inspekci do Next-Gen FW		ANO
Podpora pasivního monitorování (TAP režim)		ANO
Možnost bypass provozu Next-Gen FW funkcí při zahlcení nebo nedostupnosti		ANO
Podpora 802.1Q tagovaných rámců		ANO
Podporovaných aplikací, min. 3000		ANO
Kategorie aplikací (nebezpečné, důležité, apod.)		ANO
URL kategorií		ANO
Kategorizovaných světových URL, min. 280 milionů		ANO
Řízení přístupu k WWW - Web Usage Control (WCU)		ANO
Filtrace podle typů aplikací webových i ne-webových		ANO
Filtrace podle reputace serverů		ANO
SSL inspekce (dekrypce/enkrypce)		ANO
Security Inteligence database – známé uzly botnet sítí C&C		ANO
Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.		ANO
Možnost integrovat vlastní reputační databáze		ANO
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)		ANO
Filtry mohou zohlednit roli a identitu uživatele		ANO

Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)		ANO
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě (Network Behavior Analysis - NBA)		ANO
Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení: ☐ Operační systém Dodavatel OS ☐ Použité síť. protokoly Použité síť. služby ☐☐Otevřené porty síť. služeb ☐☐Potenciální zranitelnosti		ANO
Přehled o síťových spojení má poskytovat minimálně tyto informace: ☐ Čas startu a konce flow Akce (allow, deny,..) ☐☐Důvod případného blokování ☐ Zdrojová a cílová adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdrojový a cílový port ☐☐Aplikační protokol ☐ IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace ☐ „Business impact" aplikace ☐ Množství přenesených dat		ANO
Správa Next-Gen FW a IPS (v případě rozšíření)		
Možnost centrální správy při nasazení více firewallů		ANO
Při centrální správě: možnost sdílených bezpečnostních politik		ANO
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole) Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.		ANO ANO
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu		ANO
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole		ANO
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic		ANO
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu		ANO
V grafickém rozhraní dohledové konzole lze definovat		ANO
uživatelské dashboardy typu top-N		ANO
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů		ANO