Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.		ANO
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod. Podpora posílání událostí formou syslog, email, SNMP na externí platformy		ANO ANO
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM: ☐ ArcSight ☐ BMC Remedy Trustwave NetForensics Novell Sentinel ☐☐Hawk Network Defense Q1Labs-QRadar ☐☐☐og Rhythm SIEM 2.0 LogLogic ☐☐Splunk		ANO
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay		ANO
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu		ANO
Podpora řízeného přístupu podle rolí administrátorů		ANO
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora		ANO
Možnost založit pro daný incident „ticket" přímo v prostředí GUI managementu		ANO
Workflow pro předávání „ticketů" mezi administrátory		ANO
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu" pro další analýzu		ANO
Možnost definice politik pro sledování odpovídajících parametrů „zdraví" na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)		ANO
Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví"		ANO
Různé politiky pro sledování „zdraví" lze aplikovat na různé senzory nebo centralizovanou konzoli		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		ANO

základě zaregistrování čísla aktivovaného servisního záručního kontraktu.		
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

Ve spojení s centralizovaným managementem tyto bezpečnostní služby získávají funkce „Next-Generation" FW (dále jenom NGFW) a IPS a disponují tak možnostmi detekce a potlačení pokročilých a cílených typů útoků. Tyto, a další, mechanismy jsou explicitně vyžadované ve specifikacích vyhlášky zákona 181/2014 Sb. o kybernetické bezpečnosti:

- *§17 Nástroj pro ochranu integrity komunikačních sítí*
- *§20 Nástroj pro ochranu před škodlivým kódem*
- *§22 Nástroj pro detekci kybernetických bezpečnostních událostí*
- *§23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí*
- *§24 Aplikační bezpečnost*
- *§26 Nástroje pro zajištění vysoké úrovně dostupnosti*

Ve spojení s používaným a plánovaným řešením pro centralizované řízení a monitorování přístupu do sítě (LAN, WiFi, VPN) podle kontextu (detailní znalost o uživateli a přístupové platformě) lze reagovat i na požadavky:

- *§18 Nástroj pro ověřování identity uživatelů*
- *§19 Nástroj pro řízení přístupových oprávnění*

Klíčové nové vlastnosti takto rozšířených NGFW jsou:

- IPS nebo IDS detekční a ochranný systém se schopností automatického ladění souboru IPS/IDS signatur podle sledování prostředí a automatickým vyhodnocením stupně nebezpečnostní útoků v relevanci s metodou útoku a zranitelností cílového systému
- Automatické potlačení útoku (Remediation) na základě korelace událostí s nastavenými pravidly pro odpovídající typy reakce (např. signalizace

požadavku směrem do jiných síťových zařízení pro odpojení stanice, nastavení přístupového filtru, přesměrování apod.)

- Interní korelace událostí (typ útoku, komunikace v botnet síti, přenos malware, apod.) pro automatickou detekci kompromitovaných stanic
- Kontinuální analýza síťového prostředí s automatickou reakcí na porušení pravidel (compliancy) – např. detekce nepovoleného OS v určitém segmentu sítě, vybočení ze „standardního" obrazu komunikace apod.
- Detekce přenosu malware, včetně zero-day typů souborů, s možností retrospektivního monitorování (trajektorie přenosu souborů sítí: první stanice která soubor získala, protokoly a metody přenosu v rámci sítě, reakce senzorů nebo agentů na koncových stanicích na daný malware, apod.)
- Aplikační firewall s možností definice vlastních aplikací (podpora OpenAppID aplikačních signatur)
- URL filtrace podle web kategorií, reputace, konkrétních URL
- Integrace Security Intelligence blacklistů – DNS, URL, známé adresy botnet sítě, problematické stroje v Internet
- Antimalware ochrana – analýza přenášených souborů s možností dynamické analýzy a sandboxing se záznamem přenosu všech souborů sítí pro následnou retrospektivní analýzu

Služby NGFW a její komponenty se spravují na fyzickém nebo virtualizovaném zařízení. Pro kompletní komunikaci administrátorů s centralizovaným managementem (analýza komunikace, bezpečnostních událostí, kontextová viditelnost atd.) je k dispozici plně webové GUI. Není potřeba žádný klientský SW.

- Veškeré dashboardy lze modifikovat
- Na základě korelace bezpečnostních incidentů jsou pro všechny stanice v síti poskytovány tzv. indikátory kompromitace (IoC).
- NGFW disponuje funkcí učení se prostředí pomocí strojového učení (machine learning) a korelací se znalostní databází dodavatele) poskytuje rychlý a názorný pohled na trendy, typy komunikací, stanic, událostí atd. v síti.
- Provoz, který je řádkem pravidla firewallem explitně propuštěn může být dále kontrolován detekčními systémy IPS/IDS, systém umožňuje dále analyzovat přenášené soubory pomocí služby pokročilé ochrany před malwarem, sledovat zdraví, monitorovat prostředí, atd.
- NGFW API dovoluje integraci se systémy SIEM, log servery apod.
- Centralizovaný management integruje i reportovací systém. K dispozici jsou hotové šablony, přičemž lze definovat i vlastní obsah reportů (grafické dashboardy, tabulky, grafy apod.)

2.13. Virtuální privátní sítě, vzdálené přístupy do sítě

Suplikant, který centralizuje, sjednocuje a zabezpečuje kontrolu přístupu do sítě na základě bezpečnostních politik pro koncové uživatele připojené přes kabelové, bezdrátové sítě nebo

VPN. Poskytuje rozsáhlou viditelnost a přesnou identifikaci pomocí profilování koncových zařízení čím přispívá k snížení počtu neznámých koncových bodů v síti. Zjednodušuje možnosti připojení pro hosty do Guest sítě a jejich správu prostřednictvím plně přizpůsobitelných mobilních nebo desktop portálů. Urychluje BYOD a Enterprise Mobility se snadným „out-of-the-box" nastavením a správou certifikátů pro interní zařízení, všechno s jednotným a přehledným managementem. Umožnuje automaticky reagovat na bezpečnostní hrozby prostřednictvím integrace s NGFW, kde řešení pro kontrolu přístupu do sítě na základě sdílených informací může infikované koncové zařízení pozorovat, omezit mu přístup, nebo napomoci v remediačním procesu.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 5300	5300ks (lic)	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	L-AC-PLS-LIC L-AC-APX-LIC	
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/anyconnect-secure-mobility-client/index.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Podpora SSL VPN I IPSec VPN Ipsec VPN s podporou atabase: 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 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 Podpora šifrovacích algoritmů elyptických křivek (součást Suite-B): ECDH, ECDSA		ANO
Jednotný klient pro Ipsec (IKEv2) I SSL VPN 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
Distribuce VPN klient SW může poskytnout I jednotný 802.1X supplicant s autentizačními metodami: EAP-TLS, tunelovaný EAP-TLS, EAP-MSCHAPv2 nebo EAP-GTC, chráněný pomocí EAP-PEAP, EAP-FAST nebo EAP-TTLS VPN klient může být distribuovaný s 802.1X ataba 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 ataba mobilní atabase na bázi Android a Apple iOS.		
Podora TLS I DTLS pro SSL připojení Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. V AD)		ANO
Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu atabase a operačního systému Podpora clientless SSL VPN přístupu s pluginy pro aplikace (např. Ssh, RDP, VNC), zpřístupnění interních webových aplikací, souborů sdílených přes CIFS, přístup na aplikace pomocí port forwarding nebo pomocí tenkého klienta na úrovni appletu		ANO
Podpora autentizačních mechanizmů: lokální atabase 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 Podpora veřejných CA, včetně možnosti CA přímo na firewallu		ANO
Možnost současné autentizace AAA a certifikátem Podpora CRL a OCSP pro kontrolu revokace certifikátu		ANO
Podpora SSO metod: KCD, Netegrity, ClearTrust, SAML, NTLM/FTP/CIFS pass-through, HTTP pass-through pomocí formuláře; HTTP-POST pomocí substitucí proměnných Podpora Ipv6 adresních rozsahů a přiřazení Ipv6 adres klientům v případě dual-stack přístupu přes Ipv4 infrastrukturu		ANO
Podpora čistého Ipv6 přístupu na VPN koncentrátor Možnost jednotné správy přístupu uživatelů přes VPN ale I lokálně na LAN a WiFi		ANO
Klient musí umožňovat Instalaci jednotlivých svých modulů, které dovolí integraci a viditelnost pro uživatele následujích bezpečnostních řešení poptávaných v jiných částech: ☐ Pokročilá ochrana proti malware pro koncové body ☐☐Řízení přístupu k síťovým prostředkům (802.1x) ☐ Ochrana emailové komunikace ☐ Ochrana webové komunikace prostřednitvím webové brány ☐ Ochrana webové komunikace prostřednitvím DNS		ANO ANO 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

2.14. Přístupové přepínače s 24 PoE porty

LAN L3 přepínač s 24x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Slouží jako přístupový přepínač pro připojení zařízení jako jsou uživatelská PC a tiskárny. Je to nedílná součást řízené skupiny a virtualizované platformy nad sítí, kdy veškerý provoz na něm bude plně směrován pomocí VxLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, které umožnuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 80	80ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9300-24P-A	
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/switches/catalyst-9300-24p-a-switch/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**

Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO
Napájecí stohovací kabel požadován		ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Minimální PoE budget	430W	ANO
Uplink porty	8x10GE SFP+	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
IEEE 802.3ad (Link Aggregation)		ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis Minimálně 8 linek jako součást Link Aggregation Group trunku		ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x		ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)		ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)		ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů		ANO
RADIUS CoA		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Směrování protokolů IPv4 a IPv6 v hardware		ANO
OSPFv2		ANO

OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
Reverse path check (uRPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VACL		ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP		ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IEEE 802.3af		ANO
IEEE 802.3at		ANO

IEEE 802.3az		ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šifrovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (iPXE) pres IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		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

2.15. Distribuční přepínače

LAN L3 přepínač s 48x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Prvek je v roli hraničního přepínače, který slouží jako lokální podřízený síťový kontroler zajišťující konektivitu do WAN a management řízených skupin a virtualizované platformy nad sítí. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, které umožnuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 73	73ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9300-48P-A	
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/switches/catalyst-9300-48p-a-switch/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**

Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO
Napájecí stohovací kabel požadován		ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Počet portů 1/2.5/5/10 Gbase-T s PoE napájením		ANO
Minimální PoE budget	430W	ANO
Uplink porty	8x10GE SFP+	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
IEEE 802.3ad (Link Aggregation)		ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis Minimálně 8 linek jako součást Link Aggregation Group trunku		ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x		ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)		ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)		ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů		ANO
RADIUS CoA		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Směrování protokolů IPv4 a IPv6 v hardware		ANO

OSPFv2		ANO
OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
Reverse path check (uRPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VACL		ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP		ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IEEE 802.3az		ANO

Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šifrovaného datového provozu		ANO
Analýza šifrovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (iPXE) pres IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		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

2.16. Přístupové přepínače s 48 PoE porty

LAN L3 přepínač s 48x 1Gb/s POE porty a 8x 10Gb/s SFP+ porty. Slouží jako přístupový přepínač pro připojení zařízení jako jsou uživatelská PC a tiskárny. Je to nedílná součást řízené skupiny a virtualizované platformy nad sítí, kdy veškerý provoz na něm bude plně směrován pomocí VxLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, které umožnuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 72	72	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9300-48P-A	
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/switches/catalyst-9300-48p-a-switch/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**

Typ přepínače	L2/L3 přepínač	ANO
Formát přepínače	Stohovatelný	ANO
Počet dedikovaných stohovacích portů	2	ANO
Minimální počet zařízení ve stohu	8	ANO
Minimální kapacita sběrnice stohu	400 Gb/s	ANO
Sdílení výkonu napájecích zdrojů napříč celým stohem		ANO
Stateful Switch Over v rámci stohu		ANO
Non-stop Forwarding		ANO
Možnost instalovat interní redundantní napájecí zdroj		ANO
Interní redundantní napájecí zdroj požadován		ANO
Datový stohovací kabel požadován		ANO
Napájecí stohovací kabel požadován		ANO
Počet portů 10/100/1000 Base-TX s PoE napájením	48	ANO
Minimální PoE budget	430W	ANO
Uplink porty	8x10GE SFP+	ANO
Min. velikost sdíleného systémového bufferu	16MB	ANO
Velikost MAC address tabulky	30000	ANO
Min. počet IPv4 routes	32000	ANO
Min. počet IPv6 routes	16000	ANO
Min. počet konfigurovatelných security ACL	5000	ANO
IEEE 802.3ad (Link Aggregation)		ANO
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis		ANO
Minimálně 8 linek jako součást Link Aggregation Group trunku		ANO
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	ANO
IEEE 802.1Q		ANO
Minimální počet aktivních VLAN	1000	ANO
IEEE 802.1x		ANO
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)		ANO
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)		ANO
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů		ANO
RADIUS CoA		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Směrování protokolů IPv4 a IPv6 v hardware		ANO
OSPFv2		ANO

OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
Reverse path check (uRPF) pro IPv4 i IPv6		ANO
IGMPv2, IGMPv3		ANO
IGMP snooping		ANO
MLD snooping		ANO
DHCP relay		ANO
Minimální počet HW QoS front	8	ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS - Strict Priority Queue		ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 úrovně	ANO
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)		ANO
IPv6 services (Telnet, SSH, Syslog, DHCP)		ANO
IPv6 QoS		ANO
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)		ANO
IPv6 Port ACL, VLAN ACL		ANO
Možnost definovat povolené MAC adresy na portu		ANO
PACL, VACL		ANO
IEEE 802.1ae na uplink portech		ANO
IEEE 802.1ae (AES-GCM-256) na uplink portech		ANO
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy		ANO
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru		ANO
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP		ANO
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO

IEEE 802.3af		ANO
IEEE 802.3at		ANO
IEEE 802.3az		ANO
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu		ANO
Multicast DNS (mDNS) gateway		ANO
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
CLI rozhraní		ANO
Analýza šifrovaného datového provozu		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Podpora network boot (iPXE) pres IPv4 i IPv6		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		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

2.17. Centrální přepínače

LAN L3 přepínač s 48x 10Gb/s SFP+ porty. Slouží jako centrální přepínač pro připojení přístupových a distribučních přepínačů v rámci řízené skupiny a virtualizované platformy sítě, kde veškerý provoz na něm bude plně směrován pomocí VxLAN enkapsulace. Přepínač podporuje plnohodnotnou integraci služby na rozpoznávání identity, která umožnuje dělit uživatele do definovaných skupin s definovanými pravidly vzájemné interakce. Přepínač podporuje analýzu šifrovaného provozu, která umožňuje zachytávat závadný kód již na síťové úrovni a významně tak přispět k zabezpečení veškeré komunikace.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 6	6ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C9500-48X-A	
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/catalyst-9500-series-switches/data_sheet-c78-738978.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**

Typ přepínače	L2/L3 přepínač	ANO
Minimální počet neblokovaných portů 1/10GE s volitelným fyzickým rozhraním typu SFP+	40	ANO
Uplink porty	8x10GE SFP+	ANO
Interní redundantní napájecí zdroj		ANO
Min. velikost sdíleného systémového bufferu	64MB	ANO
Velikost MAC address tabulky	64000	ANO
Min. počet IPv4 routes	64000	ANO
Min. počet IPv6 routes	32000	ANO
Min. počet konfigurovatelných security ACL	18000	ANO
Flexibilní alokace SRAM a TCAM zdrojů		ANO
IEEE 802.3ad (Link Aggregation - LAG)		ANO
Minimální počet aktivních VLAN	4000	ANO
IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Podpora instance spanning-tree protokolu per VLAN		ANO
Podpora jumbo rámců (min. 9198 bytes)		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
OSPFv2, OSPFv3		ANO
ISIS		ANO
BGPv4		ANO
Graceful Insertion and Removal		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Min. počet oddělených (nezávislých) směrovacích tabulek	10	ANO
MPLS VPN		ANO
MPLS VPN - 6VPE		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6		ANO
Reverse path check (uRPF)		ANO
Minimální počet HW QoS front	8	ANO
QoS - Strict Priority Queue		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS Policing		ANO
QoS-Per Flow policing		ANO
QoS-Hierarchical QoS	2 úrovně	ANO
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)		ANO
IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard)		ANO
Port ACL, VLAN ACL		ANO

Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů		ANO
Podpora SUDI (IEEE 802.1AR) autentizace		ANO
IPv6 Port ACL, VLAN ACL		ANO
IEEE 802.1AE na všech portech		ANO
Source-Group Tag Exchange Protocol nebo ekvivalentní		ANO
IGMPv2/v3 snooping		ANO
MLD snooping		ANO
Multicast DNS (mDNS) gateway		ANO
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní		ANO
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type		ANO
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX		ANO
SSHv2		ANO
Analýza šifrovaného datového provozu		ANO
CLI rozhraní		ANO
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu		ANO
Model-driven programovatelnost prostřednictvím NETCONF/YANG		ANO
Python scripting		ANO
Linux shell		ANO
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Application hosting		ANO
Aplikace softwarových záplat, nikoli povyšování celého firmware		ANO
Streaming telemetrie prostřednictvím NETCONF/XML		ANO
SNMPv2/v3		ANO
Inventarizovatelnost komponent integrovanou RFID identifikací		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
Vzdálený port mirroring (ERSPAN)		ANO
NTPv3 server		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

2.18. Agregační směrovač

Modulární agregační směrovač s vysokou propustností, který umožňuje bezpečné a šifrované připojení do WAN sítí. Prvek bude instalován jako součást virtualizované sítě, kde bude sloužit jako koncentrátor zabezpečené šifrované komunikace mezi centrálním kontrolérem a hraničními prvky v jednotlivých řízených skupinách a virtualizovaných sítí.

☐ **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-ASR1001-X/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/routers/asr-1001-x-router/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ zařízení	Směrovač	ANO
Formát zařízení	Modulární	ANO
Minimální počet osaditelných slotů moduly rozhraní v šasi	2	ANO

Povýšitelnost o 2x 10GE SFP+ bez výměny HW		ANO
Požadovaný počet portů GigabitEthernet	6x SFP	ANO
Redundantní AC napájecí zdroj (interní)		ANO
Oddělený procesor pro funkce směrování a forwardování paketů		ANO
Směrování IPv4		ANO
Směrování IPv6		ANO
Propustnost systému	2,5Gb/s	ANO
Kapacita povyšována licenčně, bez povyšování HW		ANO
Maximální dosažitelná kapacita bez povýšení HW	20 Gbps	ANO
Paketový výkon směrovače	15Mpps	ANO
Softwarová redundance routovacího procesu	povýšením licence	ANO
Funkce stavového firewallu		ANO
Stavová redundance firewallu/NAT i mezi šasi	povýšením licence	ANO
Zabezpečení přenosu metodou IPSec		ANO
Funkce klasifikace aplikací, měření jejich odezev a následná aplikace příslušných přenosových politik	povýšením licence	ANO
Nástroj správy klasifikace aplikací (ev. licence pro zařízení)	povýšením licence	ANO
Funkce NAT mezi IPv6 a IPv4	povýšením licence	ANO
Minimální počet záznamů ve směrovací tabulce - IPv4	1M	ANO
Minimální počet záznamů ve směrovací tabulce – IPv6	0,5M	ANO
IEEE 802.3ad OSPFv2		ANO
BGPv4		ANO
Podpora 4 byte AS numbers in BGP		ANO
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
GRE (Generic Routing Encapsulation)		ANO
Policy-based routing podle ACL		ANO
IP Multicast (PIM SSM, PIM SM) IGMPv2, IGMPv3 uRPF		ANO
DHCP relay		ANO
First Hop Redundancy Protokol pro IPv6		ANO
OSPFv3		ANO
MP BGP		ANO
IPv6 Multicast (MLDv1 & v2)		ANO
IPv6 Multicast (PIM SM)		ANO
IPv6 Multicast (PIM SSM)		ANO
IPv6 SLA nebo ekvivalentní technologie		ANO

uRPF pro IPv6		ANO
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels		ANO
IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie		ANO
DHCPv6 Relay		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS Shaping and Policing		ANO
Class Based and Priority queuing		ANO
Rate Limiting		ANO
Hierarchical QoS	3 úrovně	ANO
RSVP		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	50	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)		ANO
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback)		ANO
IPSec AES 256		ANO
Hardwarová akcelerace šifrování pro IPSec AES 256		ANO
IKEv2		ANO
SHA-2 (SHA-256, SHA-512)		ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke" lokalitami (např. pro IPT provoz)		ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů		ANO
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - využívané pásmo		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - odezvy aplikací		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - počty aplikačních spojení		ANO
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky		ANO
Monitorování aplikačních toků s využitím technologie NetFlow		ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP		ANO

adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód		
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX		ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní		ANO
Interní nástroje pro debugging procházejícího provozu		ANO
Management		ANO
CLI rozhraní		ANO
SSHv2		ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL		ANO
SNMPv2		ANO
SNMPv3		ANO
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Čítače paketů pro jednotlivá pravidla v ACL		ANO
Sériová konzolová linka		ANO
DNS klient		ANO
NTP klient s MD5 autentizací		ANO
Administrátorem definovatelné monitory (sady statistik) sbírané o každém přenášeném paketu		ANO
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Statistiky exportovatelné pomocí NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)		ANO
Export detekované aplikace jíž daný "flow" náleží		ANO
Nástroje pro měření dynamických parametrů a odezev v síti v libovolný okamžik, synteticky generovaným provozem (například IP SLA nebo ekvivalentní)		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Vzdálený port mirroring napříč L3 doménou (např. ERSPAN nebo ekvivalentní)		ANO
Syslog		ANO
Služby		ANO
NTP server		ANO
DHCP server		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

2.19. Hraniční pobočkové směrovače

Pobočkový modulární směrovač s 5x 1Gb/s kombo RJ45/SFP porty. Směrovač slouží jako hraniční prvek pro redundantní WAN konektivitu. Směrovač řídí záložní datové toky a skrz WAN sítě šifrovaně propojuje centrální kontrolér s distribučními prvky v jednotlivých řízených skupinách a virtualizovaných sítích.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 12	12ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C1-CISCO4331/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/routers/4331-integrated-services-router-isr/model.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ zařízení	Směrovač	ANO
Formát zařízení	Modulární	ANO

Požadovaný počet portů GigabitEthernet	5x10/100/1000 RJ45 a / a nebo SFP	ANO
Směrování IPv4		ANO
Směrování IPv6		ANO
OSPFv2		ANO
BGPv4		ANO
Podpora 4 byte AS numbers in BGP		ANO
Možnost směrování provozu dle dynamicky měřených metrik (zatížení linky, zpoždění, ztrátovost paketů, jitter)		ANO
First Hop Redundancy Protokol (např. VRRP, HSRP)		ANO
GRE (Generic Routing Encapsulation)		ANO
Policy-based routing podle ACL		ANO
IP Multicast (PIM SSM, PIM SM)		ANO
IGMPv2, IGMPv3		ANO
uRPF		ANO
DHCP relay		ANO
First Hop Redundancy Protokol pro IPv6		ANO
OSPFv3 MP BGP		ANO
IPv6 Multicast (MLDv1 & v2)		ANO
IPv6 Multicast (PIM SM)		ANO
IPv6 Multicast (PIM SSM)		ANO
IPv6 SLA nebo ekvivalentní technologie		ANO
uRPF pro IPv6		ANO
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels IPv6 over IPv4 Multipoint VPN nebo ekvivalentní technologie		ANO
DHCPv6 Relay		ANO
QoS classification – ACL, DSCP, CoS based		ANO
QoS marking - DSCP, CoS		ANO
QoS Shaping and Policing		ANO
Class Based and Priority queuing		ANO
Rate Limiting		ANO
Hierarchical QoS	3 úrovně	ANO
RSVP		ANO
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)		ANO
Minimální počet oddělených (nezávislých) směrovacích tabulek	20	ANO
Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING, VoIP gateway)		ANO
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback)		ANO
Stavový firewall		ANO

IPSec AES 256		ANO
Hardwarová akcelerace šifrování pro IPSec AES 256		ANO
Minimální propustnost směrovače při aktivovaných službách IPSec šifrování a QoS měřená pro IMIX provoz	70Mb/s	ANO
IKEv2		ANO
SHA-2 (SHA-256, SHA-512)		ANO
Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke" lokalitami (např. pro IPT provoz)		ANO
Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů		ANO
Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)		ANO
Vynucení QoS parametrů pro takto rozpoznané aplikace a skupiny aplikací - marking, garance šířky pásma pro jednotlivé aplikace, shaping, policing		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - využívané pásmo		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - odezvy aplikací		ANO
Měření statistik a výkonnostních charakteristik přenášených multimediálních, realtimových a aplikačních toků - počty aplikačních spojení		ANO
Sběr a vyhodnocování statistik a výkonnostních charakteristik multimediálních toků: využívané pásmo, odezvy aplikací, RTP statistiky		ANO
Monitorování aplikačních toků s využitím technologie NetFlow		ANO
Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód		ANO
Podpora minimálně 2 různých monitorů současně (pro monitoring bezpečnosti a monitoring objemu přenesených dat)		ANO
Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX		ANO
Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní		ANO
4G LTE záložní komunikační kanál		ANO
Interní nástroje pro debugging procházejícího provozu		ANO
SSHv2		ANO
CLI rozhraní		ANO
SNMPv2/v3		ANO
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
NTP server		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

2.20. Rozšiřující 10GB karty

Originální rozšiřující karta s 16x 10Gb/s SFP+ porty pro Cisco Catalyst 6509E osazeným Supervizorem 2T. Karta umožňuje provoz minimálně 80Gb/s na sběrnici.

☐ **Základní údaje**	**Nabízená hodnota**	
Výrobce zařízení	CISCO	
Počet kusů zařízení - 3	3ks	
Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení)	C6800-16P10G=	
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/catalyst-6800-series-switches/datasheet-c78-733662.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
typ zařízení	rozšiřující modul switche	ANO

Minimální počet 10Gb/s portů	16	ANO
Kompatibilní se šasi Cisco C6509E		ANO
Kompatibilní se supervisorem 2T a 2TXL		ANO
Rychlost komunikace se sběrnicí	80 Gb/s	ANO

2.21. Rozšiřující servisní moduly

Originální supervizor kompatibilní do šasi Cisco Catalyst 6509E s minimální propustností 2Tb/s.

☐ 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)	VS-S2T-10G=	
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/interfaces-modules/catalyst-6500-series-supervisor-engine-2t/data_sheet_c78-648214.html	
Požadovaná hodnota parametru	**Minimální požadavky**	**Splněno (ANO/NE)**
Typ zařízení	řídící modul switche	ANO
Celková minimální propustnost přepínacího subsystému	2 Tb/s	ANO
Přepínání IPv4 v Hardware	720 Mpps	ANO
Přepínání IPv6 v Hardware	390 Mpps	ANO
Minimální počet 128 000 záznamů v MAC adresní tabulce		ANO
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	256000	ANO
Minimální počet záznamů ve směrovací tabulce – IPv6 unicast	128000	ANO
Minimální počet aktivních VLAN	4000	ANO
Řídící modul s integrovanými rozhraními 10GE		ANO
Redundantní řídící modul		ANO
Neměnná propustnost i při výpadku redundantního řídícího modulu		ANO
Funkční specifikace		ANO
Virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi (jediná entita z pohledu L2 i L3 protokolů)		ANO
Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení		ANO
Podpora servisních modulů i v jednom virtuálním šasi sloučeném ze dvou fyzických		ANO

Stavové přepnutí mezi řídicími moduly v jednom fyzickém šasi (ekvivalent funkce Statefull Switchover/SSO)		ANO
Stavové přepnutí mezi řídícími moduly v logickém šasi (ekvivalent funkce Statefull Switchover/SSO mezi fyzickými šasi)		ANO
Směrování protokolů IPv4 a IPv6 v hardware (duální podpora IPv4 a IPv6, tedy možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack)		ANO
HW podpora MPLS a VPLS		ANO
Podpora tunelovacích protokolů (např. GRE) v hardware		ANO
Podpora překladu adres/NAT v hardware		ANO
Podpora standardu IEEE 802.3ad		ANO
Podpora IEEE 802.3ad přes více modulů		ANO
Podpora IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)		ANO
Minimální počet konfigurovatelných PortChannel trunků	128	ANO
Podpora IEEE 802.1Q		ANO
Podpora tunelování 802.1Q v 802.1Q		ANO
Podpora IEEE 802.1s - multiple spanning trees		ANO
Podpora IEEE 802.1w - Rapid Spanning Tree Protocol		ANO
Podpora IEEE 802.1p		ANO
Protokol MVRP nebo VTP pro definici a správu VLAN sítí		ANO
Detekce protilehlého zařízení (např. CDP nebo LLDP)		ANO
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“		ANO
Detekce jednosměrnosti optické linky (např. UDLD)		ANO
Podpora QoS classification – dle ACL, IP Prec, DSCP, CoS		ANO
Podpora QoS marking –dle IP Prec, DSCP, CoS		ANO
Podpora QoS Policing		ANO
Podpora policingu na hodnotu agregovanou ze všech karet s lokálním přepínáním		ANO
Podpora policing per-flow (např. microflow policing nebo funkčně ekvivalentní)		ANO
Podpora konfigurovatelných HW prostředků ochrany CPU před útoky typu DoS		ANO
Podpora hardwarové filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní		ANO
Podpora hardwarové filtrace (access list) dle L2, L3 i L4 informací		ANO
Podpora hardwarové filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)		ANO
Podpora klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Security Group Exchange Protocol dle RFC draft-smith-kandula-sxp-01 nebo funkčně ekvivalentní).		ANO

Podpora propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)		ANO
HW podpora IEEE 802.1ae na 1 Gbit/s i 10 Gbit/s portech		ANO
Podpora zabezpečení a analýzy DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)		ANO
Podpora ochrany ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní)		ANO
Podpora ochrany podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)		ANO
Podpora MPLS směrování		ANO
Podpora VPLS směrování		ANO
Podpora BGPv4, MP-BGP		ANO
Podpora OSPFv2, OSPFv3		ANO
Podpora OSPF s MD5 a NSSA		ANO
Podpora RIPv2, RIPng		ANO
Podpora IS-IS podpora pro IPv4 a IPv6		ANO
Podpora Router Redundancy protokolu pro IPv4 (např. VRRP, HSRP)		ANO
Podpora Policy-based routing podle ACL		ANO
EIGRP (dle RFC draft-savage-eigrp-01)		ANO
Podpora PIM-SM (Protocol Independent Multicast, sparse mód)		ANO
Podpora PIM SSM (PIM Source Specific Multicast)		ANO
Podpora Bidirectional Protocol Independent Multicast (RFC 5015)		ANO
Podpora IGMPv2, IGMPv3		ANO
Podpora antispoofingové kontroly ekvivalentní funkci RPFC, reverse path forwarding check dle RFC3704 a RFC3178 pro IPv4 i IPv6		ANO
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)		ANO
Podpora IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP)		ANO
Podpora Router Redundancy protokolu pro IPv6 (např. VRRP, HSRP)		ANO
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery)		ANO
Podpora IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)		ANO
Podpora IPv6 over GRE v hardware		ANO
Podpora ISATAP v hardware		ANO
Podpora IPv6 QoS		ANO
Možnost vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkční ekvivalent Virtual Routing and Forwarding/Multi-VRF)		ANO

Podpora protokolů a služeb per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)		ANO
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6		ANO
Podpora NetFlow (nebo funkčně ekvivalentní) na vstupu i výstupu		ANO
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů		ANO
Statistiky určovány z každého paketu daného "flow"		ANO
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb		ANO
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"		ANO
Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu.		ANO
Export statistik "flow" selektivně na více kolektorů		ANO
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení		ANO
Konfigurovatelná autodiagnostika při startu i za provozu zařízení		ANO
Podpora nástroje měření odezev sítě (např. IP SLA) pro IPv4 i IPv6		ANO
Měření a ovládání spotřeby energie k LAN připojených koncových zařízení		ANO
Trasování media/aplikačních datových toků v celé síti a sběr statistik ze zařízení jimiž toky prochází		ANO
Textové řádkově orientované/CLI konfigurační rozhraní		ANO
Konfigurace zařízení v člověku čitelné textové formě		ANO
Možnost povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP		ANO
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP		ANO
Sériová konzolová linka		ANO
SSHv2		ANO
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL		ANO
Podpora synchronizace času protokolem NTPv3 (klient i server)		ANO
SNMPv2		ANO
SNMPv3		ANO
L2 traceroute		ANO
RADIUS klient pro AAA (autentizace, autorizace, accounting)		ANO
TACACS+ klient		ANO
Podpora zrcadlení portů (funkční ekvivalent SPAN)		ANO
Podpora vzdáleného zrcadlení portů (funkční ekvivalent RSPAN)		ANO
Pokročilé interní nástroje pro ladění/debugging procházejícího provozu		ANO

Interní nástroje umožňující detailní analýzu a troubleshooting procházejících multimediálních datových toků, např. mediatrace nebo ekvivalentní		ANO
Podpora Syslog		ANO
DHCP server		ANO
NTP server		ANO

2.22. Propojovací moduly

25.

Základní údaje	Nabízená hodnota
QSFP 40-Gbps bidirectional short reach tranciever	
Výrobce zařízení	CISCO
Počet kusů - 60	60ks
Produktové číslo (typ) nabízeného zařízení	QSFP-40G-SR-BD
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/interfaces-modules/transceiver-modules/data_sheet_c78-660083.html
10GBASE long reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 240	240ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-LR-S=
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/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html
10GBASE metalický SFP+ kabel 3 metry	
Výrobce zařízení	CISCO
Počet kusů - 8	8ks
Produktové číslo (typ) nabízeného zařízení	SFP-H10GB-CU3M=
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/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html
10GBASE short reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 8	8ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-SR-S=
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/interfaces-modules/transceiver-modules/data_sheet_c78-455693.html

QSFP 40-Gbps -to 4x 10G SFP+ Breakout cable 5m	
Výrobce zařízení	CISCO
Počet kusů - 4	4ks
Produktové číslo (typ) nabízeného zařízení	QSFP-4SFP10G-CU5M=
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/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/40GE_Tx_Matrix.html
1GBASE-T RJ45 metalický SFP transceiver	
Výrobce zařízení	CISCO
Počet kusů - 13	13ks
Produktové číslo (typ) nabízeného zařízení	GLC-TE=
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/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/GE_Tx_Matrix.html
10GBASE long reach SFP modul	
Výrobce zařízení	CISCO
Počet kusů - 10	10ks
Produktové číslo (typ) nabízeného zařízení	SFP-10G-ZR-S=
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/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/10GE_Tx_Matrix.html
Třída zařízení optický transceiver	ANO
Formát zařízení výměnný modul	ANO
Rychlost 10Gb	ANO
Dosah 80km	ANO
optický mód SMF	ANO
Vlnová délka světla 1550 nm	ANO
teplotní rozsah standard	ANO
konektor vlákno Dual LC/PC	ANO
konektor box GLC	ANO

3. Instalace a implementace Bepečného síťového prostředí

Dodavatel dále samostatně provede, dle závazného harmonogramu a schváleného postupu – anylýzy Detailního návrhu řešení, tyto činnosti:

A.) Instalace zařízení v jednotlivých lokalitách

- Bude postupováno dle Zadavatelem schváleného Detailního návrhu řešení
- Bude postupování dle Zadavatelem schváleného harmonogramu

B.) Implementaci řešení, dle jednotlivých etap 3. až 8.

- Bude postupováno dle Zadavatelem schváleného Detailního návrhu řešení
- Bude postupování dle Zadavatelem schváleného harmonogramu

A.) Instalace zařízení v jednotlivých lokalitách – seznam lokalit

Instalace do prostředí Zadavatele začně na základě akceptovaného a předaného Detailního návrhu řešení. Lokality, ve kterých bude probíhat implementace:

ID lokality	Název lokality	Adresa
BOH	DSA - STK Bohdalec	Nad Vršovskou horou 88/4
BREV	DSA - STK Břevnov	Radimova 39, Praha 6
BUB	Archiv Bubny	Bubenská 8a
DC1	DC1 - VEGACOM	Lužná 4/591, Praha 6
DUM	Dům národních menšin	Vocelova 3, Praha 2
EMA	OMI Emauzy	Vyšehradská 55, Praha 2
CHAR	MHMP - ZSP	Charvátova 9/145, Praha 1
JAR	DSA - STK Jarov / Osiková	Osiková 2688/2, Praha 3
JUN	MHMP - Škodův palác	Jungmannova 25, Praha 1
KLA	MHMP - Clam-Gallasův palác	Mariánské nám. 3
KON	DSA - KCP (Kongresové Centrum Praha)	Na Pankráci 1685/17, Praha 4
MKP	Městská knihovna v Praze (MKP)	Mariánské nám. 1
NR	MHMP - Nová radnice	Mariánské náměstí 2, Praha 1
NUB	MHMP - Nová úřední budova	Nám. Franze Kafky 1, Praha 1
OPLET	MHMP - Opletalova	Opletalova 22, Praha 1
RAB	MHMP Radniční blok (minuta)	U Radnice
REZ	MHMP - Primátorská rezidence	Mariánské nám. 1
RYT	MHMP Rytířská	Rytířská 10, Praha 1
STR	MHMP-Staroměstská radnice	Staroměstské náměstí 1/4
VAL	MHMP - Valentinská	Valentinská 4
VYS	DSA - STK Vysočany	Na výběžku 688/11, Praha 9

B.) Implementace dle jednotlivých etap

Etapa č. 3 – Migrace DC1

- v rámci této etapy dojde k vybudování nové infrastruktury paralelně vůči stávající DC infrastruktuře
- dojde k začlenění do stávající Cisco ACI infrastruktury v DC4
- bude nainstalován systém pro analýzu datových toků
- bude nainstalován systém pro ověřování uživatelů přistupujících do sítě MHMP
- bude nainstalován systém pro management aktivních prvků
- bude nainstalován systém SDN pro přízení přístupových přepínačů (DNA center)
- následně proběhnou testy funkčnosti
- poté budou migrovány servery a služby do nové infrastruktury
- dojde k začlenění bezpečného rozhraní pro analýzu síťového provozu do DC4 a DC5

Etapa č. 4 – Migrace lokality NUB

- v prvním kroku dojde k upgradu stávajících zařízení, které budou dále využívány v nové infrastruktuře
- následně dojde k přepojení přístupových přepínačů v lokalitě a zapojení do upgradovaných páteřních přepínačů

Etapa č. 5 – Migrace lokality JUN

- v prvním kroku bude zprovozněn pár páteřních přepínačů a ty budou propojeny do lokality NUB
- následně dojde k přepojení přístupových přepínačů v lokalitě a zapojení do nových páteřních přepínačů

Etapa č. 6 – Migrace lokalit WAN

- budou nainstalovány a zprovozněny centrální směrovače a agregátory šifrovaných spojení. Zařízení budou umístěna v DC1 a lokalitě NUB (nebo jiné momentálně vhodnější – např. DC4)
- v každé z migrovaných lokalit bude nejprve instalována bezpečnostní brána – směrovač a připojena k centrálním VPN agregátorům
- následně dojde k přepojení přístupových přepínačů v lokalitě a zapojení do nových směrovačů

Etapa č. 7 – Migrace lokalit FO

- v prvním kroku bude zprovozněn přepínače s přímým optickým propojem do lokality NUB
- bude nakonfigurováno zabezpečení optických linek protokolem 802.3ae
- následně dojde k přepojení přístupových přepínačů v lokalitě a zapojení do nových páteřních přepínačů

Etapa č. 8 – Migrace perimetru

- budou definovány vazby mezi připojením perimetr segmentů a novou částí infrastruktury
- proběhne rekonfigurace komunikačních tras
- proběhne přesun ISP konektivit do cílových umístění (DC3 a NUB – nebo dle aktuálních potřeb)

- bude nakonfigurována HA topologie mezi DC i mezi ISP
- Bude provedena rekonfigurace stávajících bezpečnostních technologií

Testy

- budou provedeny akceptační testy
- budou provedeny zátěžové testy
- budou provedeny testy redundance

4. Úpravy konfigurací současných bezpečnostní technologií

V reakci na provedené úpravy v síti DC HMP bude nezbytné provést specifické úpravy ve stávajících součástech bezpečnostní infrastruktury HMP. Tyto změny budou znamenat zejména integraci již existujících bezpečnostních komponent s novými prvky sítě a napojení na nová poskytovaná rozhraní pro monitoring síťového provozu. Důležitou součástí je také zcela nová integrace nových síťových komponent do procesu sběru logů a bezpečnostního monitoringu.

- 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

Tabulka detailních požadavků na dodávané řešení úpravy konfigurací současných bezpečnostní technologií:

Parametr	Požadovaná hodnota	Nabízená hodnota (Popis)	Splňuje Ano/Ne
Perimetrové firewally společnosti Checkpoint	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Změnách v bezpečnostní politice - Úpravách/změnách kabelového zapojení zařízení	V rozsahu požadavku.	ANO
Systémy řízení a sledování přístupů k síti, DDI a Network Visibility Module NOVICOM	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Změnách v bezpečnostní politice - Úpravách/změnách kabelového zapojení zařízení	V rozsahu požadavku.	ANO

Systémy aplikačního balancování a ochrany F5	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Změnách v balancovací a bezpečnostní politice - Úpravách/změnách kabelového zapojení zařízení	V rozsahu požadavku.	ANO
Systém správy logů z provozní a bezpečnostní infrastruktury LogManager	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Změnách v konfiguraci logování - Úpravách/změnách kabelového zapojení zařízení - Zapojení dalších zdrojů logů	V rozsahu požadavku.	ANO
Nástroje pro detekci a vyšetřování kybernetických incidentů FIDELIS	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Úpravách/změnách kabelového zapojení zařízení - Zapojení na nové rozhraní pro generování dat o síťovém provozu	V rozsahu požadavku.	ANO
Nástroje pro správu bezpečnostních událostí SIEM IBM QRADAR	V souvislosti provedených změn při implementaci bezpečné sítě a všech jejích komponent zajistí dodavatel podporu při: - Úpravě definic síťových segmentů - Úpravách/změnách kabelového zapojení zařízení - Zapojení na nové rozhraní pro generování dat o síťovém provozu	V rozsahu požadavku.	ANO

5. Poskytnutí služeb podpory výrobců technologie

Zařízení v rámci dodávky jsou rozdělena do servisních kategorií, dle délky záruky a reakční doby na výpadek.

Kategorie	Počet měsíců záruky	SLA
Servisni skupina 1	36	8/5 NDB fix
Servisni skupina 2	48	8/5 NBD fix

Datum zahájení poskytování záruky je rovno datumu akceptace zařízení do provozu.

Podpora výrobce zahrnuje dostupnost:

- Upgrade, Update operačního systému a bezpečnostních aktualizace,
- Poskytování nových verzí a opravných balíčků SW, dle aktuální technologické úrovně,
- Výměna vadného dílu – odeslání NBD (následující pracovní den).

Druhy zařízení a servisní skupiny

Druh zařízení	Servisní skupina
Bezpečné rozhraní pro analýzu síťového provozu	Servisni skupina 1
Bezpečnostní hraniční brány firewall pro sítě Mepnet	Servisni skupina 1
Centrální kontrolér LAN sítě	Servisni skupina 2
Monitorování datových toků	Servisni skupina 2
Řízení přístupu k síťovým prostředkům (802.1x)	Servisni skupina 2
Správa síťového prostředí	Servisni skupina 2
Datacentrové řešení Spine-Leaf	Servisni skupina 2
Spine vrstva	Servisni skupina 2
Leaf vrstva – 10GB SFP+	Servisni skupina 2
Leaf vrstva 10GB – RJ45	Servisni skupina 2
Leaf vrstva 1GB – RJ45	Servisni skupina 2
Next-Generation Firewall	Servisni skupina 2
Virtuální privátní sítě, vzdálené přístupy do sítě	Servisni skupina 2
Přístupové přepínače s 24 PoE porty	Servisni skupina 2
Distribuční přepínače	Servisni skupina 2
Přístupové přepínače s 48 PoE porty	Servisni skupina 2
Centrální přepínače	Servisni skupina 2
Agregační směrovač	Servisni skupina 2
Hraniční pobočkové směrovače	Servisni skupina 2
Rozšiřující 10GB karty	Servisni skupina 2
Rozšiřující servisní moduly	Servisni skupina 2
Propojovací moduly	Servisni skupina 2

6. Poskytnutí školení a servisní podpory spojené s provozem technologie

6.1. Školení pracovníků Zadavatele

- Předmětem veřejné zakázky je rovněž provedení školení pro administrátory Zadavatele k používání a správě technologií dodaných v rámci této veřejné zakázky.
- Školení 3 administrátorů v celkovém rozsahu 24 hodin/osoba. Školení musí proběhnout v sídle Zadavatele, certifikovaným pracovníkem.
- Za organizační zajištění školení zodpovídá dodavatel. Zadavatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti.

6.2. Služby servisní podpory

- Podpora certifikovaného konzultanta a technika, pro řešenou oblast podpory
- Poskytování služby HotLine/Helpdesk včetně servisní technické podpory dle parametrů SLA sjednaných touto Smlouvou. Příjem požadavků přes email, telefonní linku a webové rozhraní.
- Poskytování poradenských služeb prostřednictvím HotLine/Helpdesk při řešení běžných provozních problémů správců informačních systémů v pracovní dobu, tj. v pracovní dny od 8:00 – 18:00 hodin.

Řešení a kategorie vad:

- **Vady kategorie A (kritická):**
  Vady, které způsobují provozní problémy a neumožňují využívání systémů k účelu, jemuž jsou určeny.
- **Vady kategorie B (vysoká):**
  Méně závažné vady a nedostatky, které funkčně nebo kapacitně omezují využívání systémů k účelu, ke kterému jsou určeny.
- **Vady kategorie C (střední a nízká):**
  Vady a nedostatky, které neomezují využívání systémů k účelu, ke kterému jsou určeny, ale nejsou v souladu se správnou funkcí systému.

Garance	**Vada kategorie A (režim 24x7)**	**Vada kategorie B (režim 8x5)**	**Vada kategorie C (režim 8x5)**
Potvrzení příjmu požadavku a oznámení jména řešitele zákazníkovi	Do 30 minut od okamžiku nahlášení vady.	Do 30 minut od okamžiku nahlášení vady.	Do 1 hodiny od okamžiku nahlášení vady.

Vady mohou být nahlášené buď přes záznam v helpdesku poskytovatele, nebo hlášením z monitoringu proaktivně vedeného Poskytovatelem.

6.3. Zpracování dokumentace

- Součástí předání dokončeného díla bude elektronicky zpracovaná dokumentace a zakreslení skutečného provedení.

7. Poskytování dalších odborných služeb

Jedná se o další odborné služby nezahrnuté pod písm. a) či b) odst. 1.1 Smlouvy, které budou hrazeny na základě skutečně provedené práce vyjádřené v člověkodnech.

- Školení dle požadavků Objednatele nad sjednaný rozsah.
- Konzultační podporu v rozsahu, ve kterém si to Objednatel objedná.
- Součinnost při řešení systémových problémů systémů třetích stran.
- Součinnost při implementaci systémů třetích stran.
- Spolupráce při tvorbě koncepce dalšího rozvoje bezpečné sítě Objednatele.
- Spolupráce při koordinaci třetích stran.
- Jakékoliv úpravy a funkční doplnění projektu, nad rámec zadavací dokumentace, dle požadavků a pokynů Objednatele.

8. Harmonogram

Postup implementace

Zadavatel požaduje, aby dodavatel pracoval s projektovým řízením, dle jedné z obecně uznávaných metodik projektového řízení a pro celý průběh projektu bude stanoven řídící výbor. Priority jednotlivých oblastí budou přezkoumány, dle aktuálních potřeb, neboť v některých lokalitách je situaci zastaralých technologií nutné řešit přednostně. Etapy 6 až 8 lze realizovat v libovolném pořadí, v případě, že to zdroje dovolí, lze také paralelně.

Návrh harmonogramu

Dokončení projektu bude provedeno do 12 měsíců od podpisu smlouvy s dodavatelem. Financování zakázky bude přizpůsoben tomuto návrhu harmonogramu, tj. dílo bude financováno ve třech dílčích etapách. Jednotlivé etapy nemusí být realizovány v uvedeném pořadí, lze je přeuspořádat dle požadovaných priorit organizace.

Popis dílčího plnění	Termín zahájení	Termín ukončení
Zahájení a vypracování Detailního návrhu řešení (místní šetření a prováděcí projekt), dle etapy 1 a 2.	T0	T0 + 1,5 měsíce = T1,5
Akceptace Detailního návrhu řešení zadavatelem	T1,5	T1,5 + 0,5 měsíce = T2
Dodávka softwarového a hardwarového vybavení potřebného k provozování všech požadovaných součástí, dle etap 3, 4 a 5	T2	T2 + 1 měsíc = T3
Instalace a implementace technologií dle etapy 3, 4 a 5	T3	T3 + 3 měsíce =T6
Úpravy konfigurací současných bezpečnostní technologií dle potřeb nové síťové infrastruktury dle etapy 3, 4 a 5	T2	T2 + 4 měsíce =T6
Dodávka softwarového a hardwarového vybavení potřebného k provozování všech požadovaných součástí, dle etap 6, 7 a 8	T6	T6 + 1 měsíc =T7
Instalace a implementace technologií dle etapy 6, 7 a 8	T7	T7 + 3 měsíce =T10
Úpravy konfigurací současných bezpečnostní technologií dle potřeb nové síťové infrastruktury dle etapy 6, 7 a 8	T10	T10 + 1,5 měsíce =T11,5
Autorizované školení pracovníků zadavatele a zpracování dokumentace	T10	T10 + 2 měsíce =T12
Předání dokončeného díla a elektronicky zpracované dokumentace a zakreslení skutečného provedení.	T11,5	T11,5 + 0,5 měsíce =T12
Služby podpory – záruky od výrobců technologie, skupina 1	T12	T12 + 36 měsíců =T48
Služby podpory – záruky od výrobců technologie, skupina 2	T12	T12 + 48 měsíců =T60
Poskytování technické podpory provozu dodavatelem. Podpora začíná běžet měsíc následující po předání díla – nejpozději T13.	T12	T12 + 36 měsíců =T48

Jednotlivé etapy jsou uvedeny v kalendářních měsících. To se rozumí den nabytí účinnosti Smlouvy.

9. Ostatní požadavky

Spotřební materiál a kabelážní systémy:

Součástí zakázky je také dodávka potřebného počtu všech propojovacích metalických i optických kabelů, vyvazovacích spojek a drobných úprav kabelážních systémů (např. posuny vyvazovacích panelů, pozic zařízení, atp. v rámci stávajícího datového rozvaděče, bez nutnosti porušení instalovaných optických a metalických van a patch panelů). Součástí dodávky není krimpování a vaření metalických či optických spojů do stávajících datových rozvaděčů.

V případě nabídky řešení SW formou tzv. virtual appliance (předkonfigurovaný virtuální image od výrobce daného řešení) je přípustný provoz na platformě VMware v existujícím prostředí Zadavatele, bez vícenákladů.

10. Součinnost zadavatele

- NON-IT zajištění prostor, do kterých bude nová technologie instalována
  - zálohované napájení/PDU
  - fyzický prostor v racích
  - chlazení o dostatečném výkonu
- zajištění konektivity ve směru do WAN/LAN
  - kvalita linek odpovídající normám/smluvním ujednáním
  - patch kabely s příslušnými konektory odpovídající příslušným normám či standardům
  - ponechání stávajících optických/metalických modulů pro použití v cílovém stavu (mimo lokality DC1)
- zajištění supportu pro stávající zařízení, které se zadavatel rozhodne ponechat
- zajištění součinnosti externích dodavatelů MHMP