Příloha č. 2 Kupní smlouvy - Popis funkčnosti nabízeného řešení a popis a seznam programového vybavení, zařízení a licencí potřebných pro dodávku a zprovoznění systému

1. Popis funkčnosti nabízeného řešení

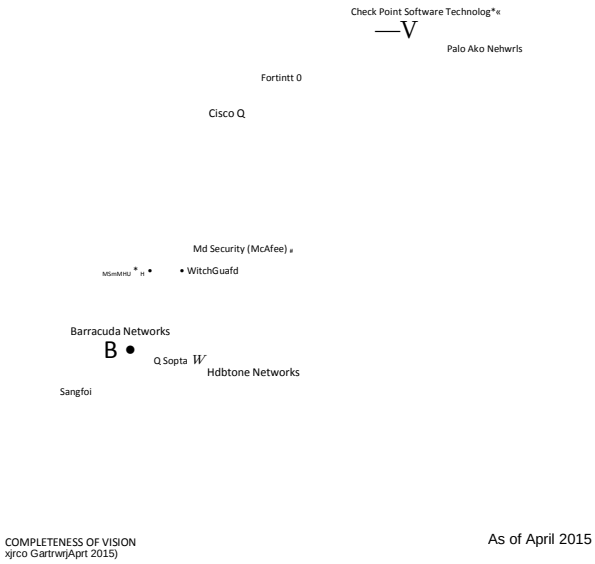
Na základě zadávací dokumentace předkládáme nabídku bezpečnostního firewallu Check Point.

Software Blade je samostatná bezpečnostní aplikace neboli modul, například firewall, VPN (Virtual Přivát Network), IPS (Intrusion Prevention System) nebo Application Control, který je nezávislý, modulární a centrálně spravovaný. Organizace tak mohou skladbu bezpečnostních prvků přizpůsobit a vytvořit si takovou kombinaci, která bude vyhovovat potřebám jejich ochrany i finančním možnostem. Software blade lze rychle aktivovat a konfigurovat na libovolné bráně nebo management systému pomocí jednoduchého kliknutí myší - nevyžaduje se žádný hardware, firmware nebo upgrade ovladačů. Když se bezpečnostní potřeby změní, lze snadno aktivovat další software blade a rozšířit bezpečnost na existující konfiguraci na stejném bezpečnostním hardwaru.

1.2. Představení technologie Check Point

Check Point Software Technologies je dlouhodobě celosvětovým lídrem v oblasti enterprise security, zaměřeným na komplexní zabezpečení sítí zákazníků. Je špičkou v oblasti IPS (první NSS Labs Recommend IPS) i Application Control a URL Filtering (největší databáze na trhu).

Produkty Check Point nabízí bezkonkurenčně nejlepší management na trhu - především díky snadné práci s politikami při jejich tvorbě, prohledávání, filtrování i sdružování. Výhodou je také přehledná a efektivní práce s logy (prohledávání a export), audit změn politik, zálohování a možnost rozšíření managementu o reporting a cross-korelační engine pro zpracovávání a vyhodnocování bezpečnostních událostí z IPS, Application Control, URL filtering, DLP, Anti-bot a antivirus.



Klíčové přínosy technologie SW Blade:

Lepší bezpečnost	Řešení s více vrstvami ochrany a konsolidovaná platforma pro podnikovou bezpečnost představuje unikátní kombinaci integrované bezpečností sítě a koncových bodů spojenou s komplexní ochranou proti malwaru.
Jednoduchost	Snadná administrace, maximální flexibilita a jednoduchá aktivace bezpečnostních prvků eliminuje složitost systému bezpečnosti; jeho provoz a údržba je celkově jednodušší.
Snadný management	Aktivace jedním kliknutím myši umožňuje rychlou implementaci bezpečnostních služeb. Centralizovaný management modulů Software Blades zvyšuje produktivitu a efektivnost.

Kompletní bezpečnost	Rozsáhlá knihovna více než třiceti Software Blades poskytuje bezkonkurenční integrované bezpečnostní řešení, které umožňuje realizovat správnou úroveň bezpečnosti na všech vrstvách sítě.
Nižší TCO	Řešení poskytuje lepší bezpečnost, možnosti rozšiřování a konsolidace, což snižuje celkové náklady na vlastnictví (TCO) v porovnání s tradičními řešeními na bázi produktů od různých dodavatelů až o 50 *%.*
Maximalizace výkonu	Kompletní škála výkonových variant zařízení - od 190 Mb/s až po 1 Tb/s. Umožňuje poskytování zdrojů při garantované úrovni služeb.
Úspory prostoru a ekologičnost	Poskytuje "Green IT" úspory na základě možnosti konsolidace více samostatných řešení a zařízení do jedné integrované brány, což redukuje nároky na prostor ve stojanu, chlazení, kabeláž a spotřebu elektrické energie.

1.3. Technické řešení

Námi navrhované řešení se skládá z dvojice bezpečnostních bran Check Point 23500-HPP (High Performance Package) zapojených v clusteru jež obsahují licenci pro 200 konkurenčních spojení klientských VPN. Systémy jsou dle požadavků zadání rozšířeny o licenci, jež umožňuje provoz 10 virtuálních instancí FW.

Management je tvořen licencí pro řízení až 25 bran a je bez dodávky FIW, tedy systém bude instalován za zařízení výrobce. Může být instalován jak na fyzický server, tak do virtuálního prostředí (např. VMware).

Sběr a korelace logů je řešena samostatně instalovanou instancí Check Point SmartEvent serveru jež je také bez dodávky FIW a systém bude instalován na zařízení výrobce. Smart Event může být instalován jak na fyzický server, tak do virtuálního prostředí (např. VMware).

Systém plně odpovídá zadávací dokumentaci a plní požadavky dle tabulky níže:

Požadavek č.	Požadovaná funkční a technická specifikace bezpečnostního firewallu	Splnění požadavku ANO/NE
1.	Dodávaná firewall platforma je ve formě samostatného hardware zařízení (fyzický FW, appliance)	ANO
2.	Dodávaná firewall platforma musí být uvedena v Gartner Magic Quadrant pro Enterprise Network Firewalls za roky 2015-2017 minimálně 2x v kvadrantu Leaders nebo Challangers	ANO
3.	Instalace do standardního 19" RACKu (Rack mount kit v ceně zařízení)	ANO
4.	Lokální FIDO, min 2x800GB RAID1, pro případ výpadku centrálního management log serveru	ANO
5.	Flot-swappable redundantní napájecí zdroje (AC)	ANO
6.	Flot-swappable redundantní ventilátory	ANO
7.	Vysoce dostupné řešení bezpečnostního firewallu s možností režimu active-standby a active-active	ANO
8.	Vyhrazené fyzické síťové rozhraní pro dohled a konfiguraci	ANO
9.	Počet požadovaných fyzických síťových rozhraní, minimálně lOx 10/100/1000baseT,	ANO

	podpora agregace fyzických interface stejného typu dle IEEE 802.3ad (bond rozhraní)	
10.	Počet požadovaných fyzických síťových rozhraní, minimálně lOx 10Gb SFP+ rozhraní, podpora agregace fyzických interface stejného typu dle IEEE 802.3ad (bond rozhraní)	ANO
11.	Možnost rozšíření: minimálně 4x 40Gb QSFP+ rozhraní	ANO
12.	Součástí dodávky bude pro každý fyzický FW 3 ks (celkem pro obě zařízení tedy 6 ks) 10GBASE-LR SFP+. Je-li použití síťových portů licencováno, musí být licence na všechny porty součástí dodávky.	ANO
13.	Propustnost Firewallu, minimálně 75 Gbps (RFC 3511, 2544, 2647,1242)	ANO
14.	Propustnost IPS, minimálně 20 Gbps (se všemi zapnutými filtry)	ANO
15.	Propustnost VPN, minimálně 14 Gbps	ANO
16.	Propustnost NGFW (Firewall, IPS, Aplikační kontrola), minimálně 20 Gbps	ANO
17.	Propustnost Threat ochrany (Firewall, IPS, Antl-Bot Aplikační kontrola, Antivir, URL filtering,), minimálně 17 Gbps	ANO
18.	Počet nových spojení za vteřinu (CPS) minimálně 200.000	ANO
19.	Počet současných spojení, minimálně 6.000.000	ANO
20.	Podpora VPN pro vzdálený přístup (IPSec, SSL), minimálně 150 současně navázaných VPN spojení / klientů, licence (je-li potřeba) pro požadovaný počet musí byt součástí nabídky	ANO
21.	Podpora Site-to-Site VPN (IPSec), minimálně 50 současně navázaných VPN tunelů, licence (je-li potřeba) pro požadovaný počet musí byt součástí	ANO
22.	Požadované funkcionality včetně potřebných licencí: firewall, ips, kontrola aplikací, url filtering, antivirus, botnet blokace, rozpoznávání uživatelských identit	ANO
23.	Podpora Duál stack konfigurace IPv4/IPv6 a to včetně konfigurace bond rozhraní a sub-rozhraní v bondu	ANO
24.	Okamžitě použitelné předdefinované IPS politiky	ANO
25.	Možnost definice IPS výjimek dle kombinace: src IP + dst IP + Service + útok/signatura	ANO
26.	Řízení politiky na základě uživatelských skupin z Active Directory	ANO
27.	Podpora transparentní Kerberos autentikace pro Single Sign On	ANO
28.	Podpora software agenta na koncové stanice pro přesné získávaní identit, bez nutnosti instalace na Windows Server, min. pro systémy Windows, s podporou ipv6, případná licence pro 5000 agentů musí být součástí nabídky	ANO
29.	Detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací 6000	ANO
30.	Možnost příchozí a odchozí FITTPS inspekce pro konkrétní virtuální firewall instanci	ANO
31.	Ochrana proti známému malwaru	ANO
32.	Funkce Blokovaní botnet komunikace na základě reputace, signatur a behaviorální analýzy	ANO
33.	Detekce a prevence DNS tunnelingu	ANO
34.	Podpora debuggování problémových scénářů na úrovni L2 - L7.	ANO
35.	Každý fyzický FW musí umožňovat vytváření a provozování virtuálních FW instancí Počet dodávaných licencí pro virtuální firewall instance minimálně 10 ks pro každý fyzický FW	ANO

36.	Počet dodávaných licencí pro dedikované virtuální prvky zabezpečující přepínaní a směrovaní (L2, L3), jsou-li potřeba nad rámec licencí pro virtuální firewall instance, minimálně 10 ks pro každý fyzický FW	ANO
37.	Load balancing virtuálních firewall instancí mezi fyzické členy active - active clusteru firewall platformy s možností kontrolovat, na kterém členu clusteru je konkrétní virtuální FW instance aktivní	ANO
38.	Podporované režimy virtuálních firewall instancí: L3 routovací a L2 transparentní režim v četně možnosti provozovat oba režimy (v různých instancích)	ANO
39.	Vytváření dedikovaných virtuálních instancí zabezpečujících přepínaní a směrovaní paketů mezi virtuálními firewally a mezi virtuálními firewally a externími segmenty.	ANO
40.	Každá virtuální firewall instance musí implementovat: vlastní bezpečnostní politiku, stavové, routovací a ARP tabulky, síťové nebo virtuální rozhraní.	ANO
41.	Řízení hardware zdrojů pro jednotlivé virtuální firewall instance (CPU, paměť)	ANO
42.	Dynamické řízení hardware zdrojů pomocí nastavení priorit pro jednotlivé virtuální firewall instance.	ANO
43.	Monitoring využívaných zdrojů pro jednotlivé virtuální firewall instance (počet spojení, využívání CPU, paměť)	ANO
44.	Možnost vypnutí IPS ochrany pro konkrétní virtuální firewall instance v případě přetížení hardware zdrojů (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu.	ANO
45.	Přímá propagace veřejných IP adres virtuálních firewall instancí ze stejného síťového rozsahu, bez nutnosti NAT-ování (virtuální L2 propoj v rámci virtualizační platformy).	ANO
46.	Kontrola síťových protokolů na aplikační vrstvě, včetně dynamického otevíraní portů pro specifický síťové protokoly (DCE-RPC, FTP, SIP, H.323, MGCP) i pro konkrétní virtuální firewall instanci.	ANO
47.	Kontrola síťových protokolů na aplikační vrstvě v případě využívaní nestandardních portů i pro konkrétní virtuální firewall Instanci.	ANO
48.	Řízení přístupu MS DCE-RPC na základě UUID 1 pro konkrétní virtuální firewall instanci.	ANO
49.	Geolokace a kontrola síťových protokolů dle zeměpisné polohy pro konkrétní virtuální firewall Instanci	ANO
50.	Aktualizace bezpečnostních signatur a geolokačních dat min. 2x týdně	ANO
51.	Management musí být fyzicky oddělený od firewall platformy - jako samostatný HW nebo jako SW appliance určená pro provoz ve virtuálním serveru. V případě, že je nutná licence pro management, musí být součástí nabídky.	ANO
52.	Konsolidovaný centrální management: správa politik a analýza logů na jedné platformě	ANO
53.	Centrální management musí umožnit připojení minimálně 10 současných uživatelů. Je-li tato funkcionalita licencována, musí být licence součástí dodávky.	ANO
54.	Centrální management systému musí umožňovat autentizaci administrátorů alespoň pomocí Microsoft Active Directory nebo RÁDIUS serveru.	ANO
55.	Funkcionalita ukládaní, filtrování a korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy	ANO
56.	Možnost vytváření uživatelsky definovatelných reportů a přehledů a jejich automatické zasílání emailem ve formátu PDF	ANO

57.	Možnost propojení se systémem SIEM třetí strany	ANO
58.	Automatická verifikace politiky (např. proti redundanci, překryvu a inkonzistenci pravidel)	ANO
59.	Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů.	ANO
60.	Podpora administrátorských profilů s možností přidělování práv (read only, red-write, none) pro jednotlivé skupiny administračních funkcí	ANO
61.	Definice oddělených politik s možností práce více administrátorů najednou (každý na přidělené politice)	ANO
62.	Možnost přidělení práv administrátorům jen pro definovanou politiku/virtuální instanci firewallu	ANO
63.	Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	ANO
64.	Fulltextové prohledávaní logů, včetně technologie indexace pro účinné a rychlé prohledávání logů/záznamů v řádu milionů	ANO
65.	Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd ...).	ANO
66.	Interní certifikační autorita za účelem vydávaní a správy PKI certifikátů pro jednotlivé firewall a VPN (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	ANO
67.	Management log server musí zpracovat min. 20000 logů/s	ANO
68.	Požadujeme historii uložených stavových informací (logů a eventů) min. 12 měsíců. Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log záznamů a eventů na management serveru (je-li disková kapacita omezena licencí, licence pro požadovanou velikost musí byt součástí nabídky), min. 16 TB	ANO
69.	Požadována licence pro centrální správu a dedikovaný reporting, minimálně pro výše požadovaný počet virtuálních firewall instancí	ANO
70.	Podpora revizí bezpečnostních politik, jejich verzování.	ANO
71.	Podpora auditních informací u změn bezpečnostní politiky.	ANO

1.4. Řízení přístupu uživatelů

Check Point kombinuje Application Control a URL Filtering Software Blades, aby sjednotil kontrolu webových aplikací s kontrolou webových stránek. Vzniká tak možnost monitorování a řízení nejen webových stránek, ale také síťových aplikací. Detekované aplikace a webové stránky jsou přehledně zobrazeny i s informacemi o uživatelích, kteří je používají. Administrátoři i management získají komplexní přehled. Organizace tak mají možnost bezpečně využívat výhody síťových i webových aplikací.

Politiky je možno vytvářet na základě adresy, jména uživatele, skupiny, zařízení nebo lokality.

Vlastnosti a výhody:

- Detekování, identifikace a řízení přístupu k webovým aplikacím, widgetům a stránkám
- Identifikace, limitování nebo blokování užívání aplikací na základě jména uživatele, skupiny či HW
- Limitování platnosti pravidel v čase (např. pracovní doba vs. přestávky)
- Vzdělávání uživatelů s pomocí UserCheck technologie
- Analýza veškerého datového toku, včetně SSL šifrované komunikace
- Appwiki - největší knihovna webových aplikací a widgetů
- Snadná integrace do architektury Softwarových Bladů
- Centrální ovládání

- Vytváření politik na základě jmen uživatelů, skupin či zařízení
- Integrace se SmartEvent Software Blade

1.5. Mobile Access blade (VPN)

Klasická funkcionalita VPN koncentrátoru pro SSL spojení ať už prostřednictvím klienta, nebo prostřednictvím webového prohlížeče.
Bude možné zajistit klienta pro přístup z desktopových i mobilních zařízení (smartphone, tablet).

1.6. Antivirus & AntiMalware - antivirový engine

Kontrola provozu proti vzorkům známých virů a malware.

- Konfigurace ochran dle jednotlivých protokolů (http, smtp, pop3, ftp)
- Konfigurace ochran dle jednotlivých typů souborů
- Konfigurace dle směru provozu
- Konfigurace výjimek
- Další nastavení (velikosti skenovaných souborů, skenování archívů, atd.).

1.7. AntiBot

Antibot je řešení, jehož úkolem je odhalit infikované stanice, zabránit další nákaze a zamezit zneužití. Vychází z Antivirus blade.

- Odhaluje infikované hostitele díky unikátnímu Multi-tier ThreatSpect TM systému
- Detekuje APT útoky a brání vzniku případných škod
- Dynamicky aktualizuje informace o útoku
- Získává Real-time bezpečnostní informace z cloudového prostředí ThreatCloud

1.8. IPS - Intrusion Prévention System

Check Point IPS Software Blade, založený na architektuře softwarových bladů, poskytuje firewall příští generace, který nabízí možnost komplexní a integrované ochrany před neoprávněným průnikem do sítě, včetně preventivní ochrany klientů, serverů a operačních systémů před hrozbami a dalšími zranitelnostmi. Check Point IPS produkty jsou podporovány službou Check Point Update Services, která nepřetržitě a v reálném čase poskytuje aktualizace a doporučení jak konfigurovat bezpečnostní politiky.

Technologie nahlíží do struktury přenášených souborů a hledá v nich potenciální hrozby. Check Point sbírá informace o chybách v aplikacích, kterých by mohl útočník využít. IPS kontroluje, zda přenášený soubor nevyužívá některé ze známých chyb k provedení útoku.

Geo-protections - IPS umožňuje nastavit bezpečnostní politiku podle oblasti. Po delším monitorování sítě se dá obvykle zjistit, že většina hrozeb přichází pouze z několika zemí. Pomocí Geo-protections je možné komunikaci s těmito oblastmi přísněji filtrovat nebo úplně zakázat.

1.9. Identity Awareness

Pro identifikaci uživatelů je využita softwarová komponenta Identity Awareness.

Autentizační metody

- Active Directory Single Sign-on (SSO)
- Browser-Based Authentication (Transparent Kerberos Authentication /Captive portal)
- Agent

1.10. Management

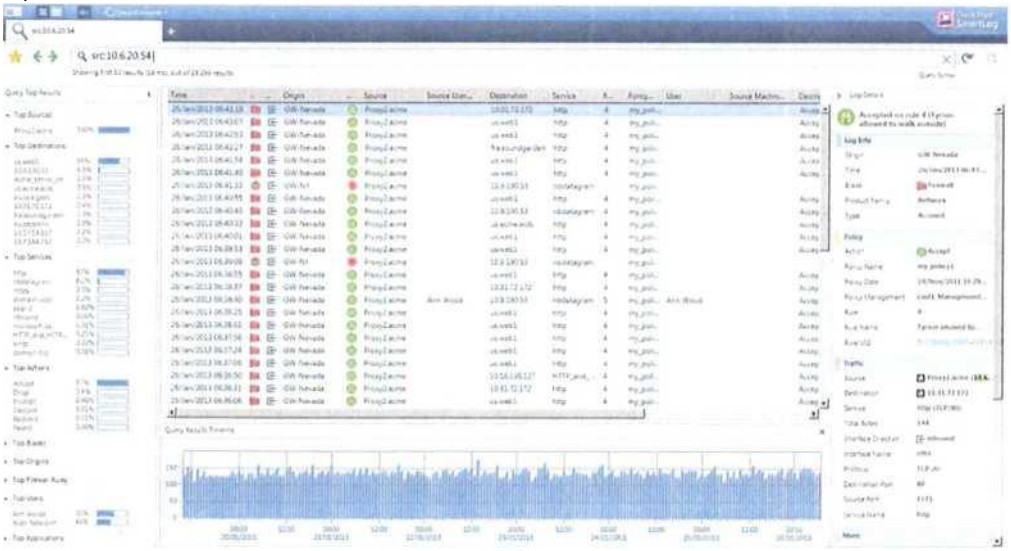
Druhá část řešení je tvořena virtuální appliance pro reporting a korelaci událostí.

https://www.checkpoint.com/products/smart-l-appliances/

Součástí managementu je také korelační jednotka SmartEvent.

1.11. Check Point SmartLog

SmartLog indexuje jednotlivé logy a poskytuje administrátorovi nástroj pro jejich velmi rychlé (díky indexaci) a přehledné zobrazení:



1.12. Check Point SmartEvent

Je analytickou nadstavbou log záznamů - zpracovává jednotlivé log záznamy, vzájemně koreluje a zobrazuje v přehledných grafech a diagramech. Celý nástroj je typu Click-and-Drill down - což znamená, že všechny výstupy (grafy, diagramy, záznamy) jsou plně aktivní a je možné se mezi nimi jednoduše proklikávat od nejobecnějšího pohledu až k nejdetailnějšímu.

1.13. Projektové řízení a popis realizace řešení

Projektové řízení budou vykonávat pracovníci, jež mají plné kompetence k realizaci díla a zároveň jsou v přímém kontaktu s odbornými pracovníky výrobce pro zajištění optimální implementační a post-implementační podpory.

Práce budou probíhat dle požadovaných projektových fází:

- Analýza aktuálního nastavení stávajícího řešení, jeho shody s platnou bezpečností politikou a potřebnosti jednotlivých nastavení včetně identifikace chybějících konfigurací.
- Představení výsledků analýzy aktuálního stavu konfigurace Firewallu zástupcům Kupujícího s cílem odsouhlasit si vstupy do přípravy cílové konfigurace.
- Příprava iniciální konfigurace odpovídající výsledkům výše uvedené analýzy aktuálního stavu s cílem plnohodnotně respektovat bezpečnostní politiku, případně další požadavky Kupujícího (v rámci funkcionalit uvedených v tomto dokumentu)
- Představení iniciální konfigurace zástupcům Kupujícího s cílem odsouhlasit si konfiguraci, která bude nastavena, testována a uvolněna do produktivního provozu
- Dodávka a instalace zařízení v místě provozovny Kupujícího
- Poskytnutí potřebné součinnosti při přípravě, provádění a vyhodnocení testů, spolupráce při opravách chyb nalezených v testech
- Zvýšená podpora při rolloutu řešení do produktivního provozu.

Pro úspěšnou realizaci je třeba zajištění součinnosti minimálně v následujícím rozsahu:

- Projektové řízení ze strany kupujcíího
- Potřebnou součinnost při analýze stávajícího stavu i návrhu cílové architektury a nastavení dodávaných produktů
- Potřebnou součinnost při dodávce a instalaci zařízení (místo, vstup, energie, konzole, VPN,...)
- Styčné osoby pro komunikaci ve věcech následné podpory L2/L3 v rutinním provozu

1.14. Záruka a podpora řešení

Záruční doba na technologie činí 12 měsíců od ukončení implementačních prací a je v rozsahu požadovaném v rámci zadávací dokumentace.

Součástí nabídky jsou pětileté licence na všechny funkcionality nabízeného řešení a poskytování servisní podpory.

1.15. Servisní podpora ICZ

Služby ICZ pro zajištění provozu zařízení čítají následující aktivity:

- držení servisní pohotovosti pro L3 podporu prostřednictvím certifikovaného technického pracovníka
- HW servis v místě instalace
- poskytnutí jednotného kontaktního místa pro hlášení a evidenci požadavků
- servisní podpora systému dle požadavků zákazníka (servisní incidenty, změna SW)
- informační servis - reakce na bezpečnostní incidenty
- poskytování Update/upgrade v rámci zakoupených licencí a podpory výrobce
- diagnostika, analýza fault/alarm a log zpráv pracovníkem ICZ
- notifikace kritických a bezpečnostních záležitostí spojených s Cisco technologiemi
- testovací aktivity pro nasazování nových služeb klienta

AIR-AP2802I-E-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE E	16	ks
AIR-AP-T-RAIL-R	Ceiling Grid Clip for Alronet APs - Recessed Mount (Default)	16	ks
AIR-AP-BRACKET-1	802.lin AP Low Profile Mounting Bracket (Default)	16	ks
SW2802-CAPWAP-K9	Cisco Aironet 2800 Series CAPWAP Software Image	16	ks
LIC-CT5520-UPG	Top Level SKU for 5520 AP Adder Licenses	1	ks
LIC-CT5520-1A	Cisco 5520 Wireless Controller 1 AP Adder License	16	ks

2.2. Bezpečnostní firewall - výrobce Check Point

Kód	Popis	Ks	Jednotka
ODDÍL 2 - Bezpečnostní firewall			
			ks
			ks
			ks
			ks
			ks
			ks
			ks

2. Seznam programového vybavení, zařízení, licencí

Předkládáme seznam dodávaného HW a SW vybavení a licencí firewallového řešení Check Point.

2.1. WiFi přístupový bod - výrobce CISCO

ODDIL 1 - WiFi přístupový bod		
CPAP-SG23500-NGTP-HPP	23500 Next Generation Threat Prevention Appliance - High Performance Package (HPP)	2
CPSB-MOB-200	Mobile Access Blade for 200 concurrent connections	2
CPSB-VS-10	10 Virtual Systems package	1
CPSB-VS-10-VSLS	10 Virtual Systems package for HA/VSLS	1
CPSM-NGSM25	Next Generation Security Management Software for 25 gateways (SmartEvent & Compliance 1 year)	1
CPSM-NGSM25-EVNT	Next Generation Security Management SmartEvent dedicated Server for 25 gateways (perpetual)	1
CPSB-NGTP-23500-1Y	Next Generation Threat Prevention Package subscription for 1 year for 23500 Appliance	8

2.3. Zprovoznění WiFi včetně bezpečnostního firewallu

ODDIL 3 - Zprovoznění WiFi včetně bezpečnostního firewallu	
Kód	Popis
	Zapojení a instalace jednotlivých komponent
	Základní konfigurace zařízení
	Rozšíření konfigurace systému
	Provedení komplexních testů
	Podrobná dokumentace
	Testovací provoz
	Akceptace díla
	Projektové řízení _____