Příloha č. 1 Kupní smlouvy Specifikace předmětu plnění

1. Obecné požadavky

Předmětem plnění této zakázky je návrh, dodávka, instalace, zprovoznění, dokumentace skutečného provedení, zaškolení administrátorů a podpora provozu nového firewallu.

Firewall musí být odolný proti výpadku jakékoliv jeho části i celé jedné poloviny bez dopadu na provoz aplikací a dostupnost dat.

Firewall bude umístěn v LAN síti Dopravního podniku Ostrava a. s.. Návrh a nabízená konfigurace musí umožňovat výhledové umístění ve dvou technických místnostech vzdálených max. 15km a to bez jakýchkoliv dalších investic, kromě výměny potřebné optické kabeláže propojující technické místnosti.

Dodavatel je povinen v rámci plnění veřejné zakázky garantovat nabízené technické parametry a doložit přesné označení nabízeného produktu včetně jeho technických parametrů pro ověření splnění požadavků Zadavatele.

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). Zboží musí být určeno pro český trh. Zadavatel požaduje potvrzení výrobce, že se jedná o zboží pro český trh. Zadavatel bude v DB výrobce uveden jako první vlastník.

Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení), že jsou určeny pro český trh.

2. Požadované technické parametry zařízení

	Požadovaná funkcionalita/vlastnost	**Splňuje ANO /NE**	**Bližší specifikace (Označení, typ, atd.)**
HW a SW parametry	2ks Next Generation Firewallů zapojených do clusteru – dále jen FW.	ANO	Check Point appliance model 6400 – viz přiložený datasheet. 6400-security-gateway-datasheet.pdf 6400-security-gateway-datasheet.pdf
	1ks zařízení pro připojení vzdálené pobočky	ANO	Check Point appliance model 1530 – viz přiložený datasheet. 1500-security-gateway-datasheet.pdf

			1500-security-gateway-datasheet.pdf
	FW musí být typu HW appliance.	ANO	viz přiložený datasheet.
	FW musí být rozměrově kompatibilní s 19" skříní (rack).	ANO	viz přiložený datasheet.
	Každý nód clusteru musí obsahovat minimálně 4 SFP+ datové porty (včetně transceiverů) o rychlosti 10Gbps s možností vytvářet na nich subinterfaces a těm přidělovat různé VLANy a další IP adresy.	ANO	10G připojení je kalkulováno v ceně.
	FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP).	ANO	LACP je podporováno.
	Možnost zálohy konfigurace FW a v případě potřeby kompletní obnova konfigurace nahráním ze zálohy.	ANO	Zálohovat a obnovovat konfiguraci lze pomocí funkce managementu anebo externího nástroje. Samotné GUI také podporuje tuto funkci.
	Pokud se FW skládá z více modulů, musí jít o moduly jednoho výrobce a tyto moduly musí být integrovány do jednoho celku s jednou, centrální správou. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW (délky platnosti licence).	ANO	Vše pochází od jednoho výrobce. Moduly jsou integrovány do jednoho celku s jednou, centrální správou. Výrobce zajišťuje požadovanou podporu.
	Nabízený FW musí být nejnovější model výrobce a nesmí mít ohlášeno datum o ukončení výroby či podpory tzn. staré modely budou ze soutěže vyřazeny.	ANO	Nabízené appliance jsou ze série Quantum uvedené v roce 2020, jedná se o novou HW řadu výrobce.
	Součástí dodávky musí být veškeré potřebné programové vybavení, tj. všechny licence potřebné pro instalaci a provoz, pro neomezený počet uživatelů a nezávislý na počtu ochraňovaných koncových systémů, nebo počtu používaných internetových doménových jmen.	ANO	Licence je kalkulována v ceně.
	Řešení musí mít funkcionalitu vysoké dostupnosti pro všechny prvky poskytující požadované funkce, s výjimkou logování a rozšířeného reportování, a to bez dalších licenčních nákladů (přípustné jsou pouze náklady na hardware).	ANO	2ks appliance v režimu HA – active/standby při využití funkce ClusterXL nepodléhá dalším licencím.

	Požadované funkcionality – Firewall, Identity Aware, Application Control, URL filtering, IPS, IPSec VPN, SSL Remote Access, Antivirus, Anti-Spyware, Clustering, cloudový Sandboxing.	ANO	V ceně jsou kalkulovány tyto funkcionality, NGTX balíček.
	Každý firewall bude mít 2ks napájecích zdrojů	ANO	Každý nabízený firewall má 2ks interních zdrojů
Požadavky na High Availability (HA) FW	FW musí používat režim HA v módu Active-Passive složený alespoň ze dvou zařízení.	ANO	Firewall tento režim podporuje.
	Veškeré informace o probíhajícím provozu musí být synchronizovány tak, aby při výpadku jednoho z boxů nedošlo k nežádoucí ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP a UDP procházejícího přes FW.	ANO	Zajištěno ClusterXL mechanismem a synchronizační linkou.
	FW musí být schopen provést failover na základě stavu jednoho ze síťových interface (up/down) nebo nedostupnosti IP adresy druhého FW v HA.	ANO	Zajištěno ClusterXL mechanismem.
Obecné minimální výkonové parametry FW (deklarovány výrobcem	Propustnost FW při zapnutí všech dostupných ochran (plné aplikační kontrole, IPS, Antivirus, URL filteringu, Anti-Spyware, Sandboxingu) a zapnutí logování musí dosahovat hodnoty alespoň 2,5Gbps (Threat prevention troughput).	ANO	2,5Gbps splňuje dle datasheetu.
	Propustnost NGFW a zapnutí logování musí dosahovat hodnoty alespoň 5Gbps.	ANO	Dle datasheetu 5,5Gbps.
	Minimální počet souběžných spojení - 990 000	ANO	2 milióny spojení dle datasheetu.
	Minimální počet nových spojení za sekundu – 53000	ANO	90 000/s nových spojení dle datasheetu.
Síťová funkcionalita FW	FW musí plně podporovat IPv4 i IPv6	ANO	Firewall je plně dual stack, podporuje jak IPv4, tak IPv6.
	FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	Firewall dané funkce podporuje. NAT je možné použít v režimech static, dynamic. PAT je podporován. NAT64 je podporován dle RFC6146.

	Možnost použití více internetových připojení v režimu active-backup nebo balancing (ECMP - Equal Cost Multiple Path).	ANO	Firewall tuto funkci podporuje. Active-Active, Active-Passive, Load balancing či load sharing režimy jsou podporovány.
	DHCP server a DHCP relay pro konkrétní sítě	ANO	Firewall tuto funkci podporuje. BOOTP a DHCP protokoly jsou podporovány.
	FW musí podporovat minimálně 20 oddělených bezpečnostních zón, mezi nimiž je možno nastavovat pravidla pro prostupy mezi zónami.	ANO	Počet security zón není omezen. Dle popisu je nejlepší zvolit technické řešení Security Groups. Tato funkce je podporována od historické verze R7X. uchazeč doporučuje nasadit nejméně verzi R80.XX.
	FW musí podporovat směrování typu Static route, RIP, OSPF, BGP a na základě politiky (Policy Based Forwarding)	ANO	Firewall tuto funkci podporuje. Podporovány jsou protokoly OSPF, BGP, PIM, RIP a IGRP.
	PBF musí být možno nakonfigurovat na základě dostupných metrik typu interface, IP adresa, zóna, uživatel.	ANO	Firewall tuto funkci podporuje. Policy based firewall je možné nakonfigurovat nejenom na základě IP address, interface, zone či objektu (uživatele), ale na mnoha dalších. Terminologie PBF je spojena s výrobcem Palo Alto.
VPN:	FW musí mít licenčně neomezený počet site-to-site VPN pomocí protokolu IPSec	ANO	Firewall tuto funkci podporuje. Řešení nemá žádné omezení na počet IPSec VPN tunelů.
	FW musí podporovat Remote Acess VPN pomocí protokolů IPSec a TLS	ANO	Firewall tuto funkci podporuje. RA VPN je dostupná pomocí protokolů IPSec, SSL i TLS.
	FW musí podporovat Clientless Remote Access VPN	ANO	Firewall tuto funkci podporuje. Clientless VPN je základ pro TLS či SSL VPN přístup.
	Počet současně připojených uživatelů musí být alespoň 1000	ANO	Technicky není omezen počet připojených uživatelů.
	Propustnost IPSec musí být alespoň 2Gbps.	ANO	2.73Gbps dle datasheetu.
Vzdálené lokality – dočasné záložní připojení	1ks zařízení pro bezpečné připojení vzdálené lokality přes VPN na 2. vrstvě (např. L2TP/IPSec)	ANO	Model 1530. Zařízení podporuje požadované funkce.

	Použije se především při výpadku primární konektivity vzdálené lokality	ANO	Uchazeč je schopen naplnit tento požadavek.
	Zařízení musí být možno přenést na kteroukoli lokalitu, a připojit tunel přes LTE nebo ethernet.	ANO	Uchazeč je schopen naplnit tento požadavek. LTE či ethernet lze použít pro VPN tunel.
	Připojení musí umožnit přenos VLAN tagů (minimálně 4 VLANy)	ANO	VLANy jsou standartně podporovány. Počet podporovaných VLAN je nejméně 1024.
Management FW	Jednotlivé HW appliance musí obsahovat grafické rozhraní (GUI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování	ANO	Managemetn Check Point GAIA OS je vždy přes zabezpečené připojení https.
	FW musí obsahovat nativní nástroj pro odchycení provozu	ANO	K dispozici Tcpdump nebo fwmonitor.
	FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	Management tuto funkci podporuje. Nelze jinak než demonstrovat.
	Out-of-band management port	ANO	Viz. Datasheet. Management tuto funkci podporuje.
Aplikační kontrola	FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	Firewall má aplikační kontrolu jako nativní funkci.
	Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	Firewall má přiřazení povolené či zakázané aplikace jako nativní součástí vytváření standardního bezpečnostního pravidla
	FW musí podporovat identifikaci aplikací na nestandardních portech	ANO	FW podporuje identifikaci aplikací na nestandardních portech.
	FW musí podporovat identifikaci aplikace napříč všemi porty/protokoly	ANO	FW podporuje identifikaci aplikace napříč všemi porty/protokoly
	Identifikace aplikace musí probíhat přímo ve FW	ANO	Identifikace aplikace probíhá přímo ve FW.
Kontrola na úrovni uživatelských identit	FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	Identity Awareness je v rámci licence.

	Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	Volba uživatelské identity jenativní součástí vytváření standardního bezpečnostního pravidla
	FW musí podporovat získávání vazby IP adresa – uživatelské jméno bez nutnosti instalace klienta na koncové zařízení.	ANO	FW podporuje získávání vazby IP adresa – uživatelské jméno bez nutnosti instalace klienta na koncové zařízení.
	FW musí podporovat vázání bezpečnostních filtrů (IPS, Webová kategorie, Antivirus, Sandboxing) na základě uživatelské identity (uživatel nebo skupina v Active Directory) a toto musí být nativní součástí vytváření standardního bezpečnostního pravidla.	ANO	FW podporuje vázání bezpečnostních filtrů (IPS, Webová kategorie, Antivirus, Sandboxing) na základě uživatelské identity (uživatel nebo skupina v Active Directory) a toto je nativní součástí vytváření standardního bezpečnostního pravidla.
	Na základě chování uživatelů, především pak surfování na internetu a C&C komunikace, musí být FW schopen vygenerovat hodnocení uživatelů a upozornit na nebezpečné uživatele.	ANO	Pomocí SmartEvent modulu v rámci licence.
	FW musí podporovat získávání vazby IP adresa – uživatelské jméno z Active Directory za pomoci doménového účtu s co nejmenšími možnými právy pro čtení security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)	ANO	FW podoruje získávání vazby IP adresa – uživatelské jméno z Active Directory za pomoci doménového účtu s co nejmenšími možnými právy pro čtení security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)
Dekrypce	FW musí podporovat dekrypci odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	Modul HTTPS Inspection s danou možností součásti licence.
	FW musí podporovat dekrypci příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	Modul HTTPS Inspection s danou možností součásti licence.
	FW musí podporovat funkci SSH proxy a kontrolovat tunelované aplikace	ANO	
	Dekryptovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	ANO	Dekryptovaný provoz je možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita

	FW musí podporovat dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	FW podporuje dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
	FW musí podporovat přeposílání dešifrovaného provozu pro potřeby archivace provozu.	ANO	FW podporuje přeposílání dešifrovaného provozu pro potřeby archivace provozu.
Cloudový Sandboxing	Sandboxing systém musí být od stejného výrobce, jako je FW	ANO	Od stejného výrobce jako FW
	Sandboxing nesmí vyžadovat žádné další HW zařízení nebo správu mimo FW	ANO	Probíha v Check Pointu ThreatCLoudu.
	Sandboxing systém musí být schopen analyzovat podezřelé soubory, a to jak přílohy v SMTP, IMAP a POP3 komunikaci, tak soubory v HTTP(S) a SMB komunikaci.	ANO	Sandboxing systém je schopen analyzovat podezřelé soubory, a to jak přílohy v SMTP, IMAP a POP3 komunikaci, tak soubory v HTTP(S) a SMB komunikaci.
	Sandboxing systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý	ANO	Sandboxing systém je schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý
	Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	ANO	Sandbox podporuje operační systémy Windows, Linux, MacOS a Android
	Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní FW	ANO	Přes SmartEvent/SmartView.
	Aktualizace zero-day signatur musí být instalována do FW v intervalu max. 5 minut.	ANO	Interval lze libovolně nastavit pro jednotlivé moduly zvlášť: IPS, AV, AntiBot.
Bezpečnostní funkcionality	FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu –povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	FW podpujeort zavedení tzv. pozitivního bezpečnostního modelu –povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu
	FW musí obsahovat integrovaný systém ochrany proti zranitelnostem a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	Aktuální databáze signatur se stahuje na Firewall.

	FW musí obsahovat antivirový engine pro skenování provozu v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	ANO	FW obsahuje antivirový engine pro skenování provozu v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB
	FW musí podporovat možnost zablokování komunikace se známými C&C servery i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	ANO	FW podporuje možnost zablokování komunikace se známými C&C servery i v případě, že je provoz šifrován a není možné provádět SSL dekrypci
	FW musí v takovém případě jednoznačně identifikovat původce C&C komunikace	ANO	FW v takovém případě jednoznačně identifikuje původce C&C komunikace
	FW musí, pro přístup ke kritickým aplikacím, poskytovat možnost vynutit více faktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje více faktorovou autentizaci.	ANO	Funkce SAML.
	FW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	FW poskytuje možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu
	FW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	FW poskytuje funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany je pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru
	Zablokování útoků typu Cross Site (XSS) a SQL injection útokům	ANO	Zablokování útoků typu Cross Site (XSS) a SQL injection útokům
	IP Geolocation Policy pro možnost povolení nebo zablokování přístupu z jednotlivých států	ANO	Geo Policy součástí Firewall policy balíčků.
	Výrobce FW se musí nacházet v kvadrantu „Leaders“ Enterprise Network Firewalls reportu společnosti Gartner v posledním aktuálním reportu	ANO	Výrobce FW se nachází v kvadrantu „Leaders“ Enterprise Network Firewalls reportu společnosti Gartner v posledním aktuálním reportu
URL filtering	FW musí obsahovat nativní podporu pro využívání databáze URL tak, aby bylo možno	ANO	FW obsahuje nativní podporu pro využívání databáze URL tak,

	zakázat určité kategorie URL (například Games, Gambling, Hacking, Sex, …)		aby bylo možno zakázat určité kategorie URL (například Games, Gambling, Hacking, Sex, …)
	FW musí podporovat vytváření administrátorsky definovaných kategorií, Allowlist, Blocklist	ANO	FW podporuje vytváření administrátorsky definovaných kategorií, Allowlist, Blocklist
	URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL vedoucích na škodlivý obsah, nebo C&C centra	ANO	URL databáze je dynamicky aktualizovaná na základě nově zjištěných URL vedoucích na škodlivý obsah, nebo C&C centra
	URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	URL databáze podporuje možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL
Logování	FW musí obsahovat logování (lokálně, a na logserver) a rozšířený reporting (vč. statistik uživatelských aktivit)	ANO	Statistiky, reporty a přehledy ve SmartEvent modulu – součást licence.
	FW musí obsahovat nástroj pro analýzu logů (zpětný náhled do logů) bez nutnosti využití dalšího systému mimo GUI	ANO	FW obsahuje nástroj pro analýzu logů (zpětný náhled do logů) bez nutnosti využití dalšího systému mimo GUI
Záruka, servis a služby	Záruka min. 5 let se servisem v místě instalace s reakcí minimálně NBD (NextBusinessDay)	ANO	Záruka je zajištěna pomocí supportu společnosti Check Point Software Technologies v požadované délce 5 let. Reakce je v režimu 8x5 NBD. Servisní požadavky je možné hlásit v režimu 24x7 non stop.
	Záruka garantovaná výrobcem	ANO	Záruka je zajištěna pomocí supportu společnosti Check Point Software Technologies v požadované délce 5 let. Reakce je v režimu 8x5 NBD. Servisní požadavky je možné hlásit v režimu 24x7 non stop.
	SW podpora výrobce minimálně 5 let	ANO	SW podpora je zajištěna pomocí supportu společnosti Check Point Software Technologies v požadované délce 5 let. Reakce je v režimu 8x5 NBD. Servisní požadavky je možné hlásit v režimu 24x7 non stop.

	Instalace, konfigurace a integrace	ANO	Instalace, konfigurace, integrace a projektové řízení nasazení firewallu je součástí nabídky a je kalkulováno v nabídkové ceně.
	Zaškolení obsluhy	ANO	Zaškolení obsluhy je součástí nabídky a je kalkulováno v nabídkové ceně.

V Praze dne:

……..…….……..…

Pavel Šipr
Jednatel

V Ostravě dne:

……..……..

xxx
Vedoucí odboru ICT