Zmluva o dielo č. Z20235407_Z

uzatvorená v zmysle §536 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Exportno-importná banka Slovenskej republiky, skrátene EXIMBANKA SR
Sídlo:	Grösslingová 1, 81109 Bratislava, Slovenská republika
IČO:	35722959
DIČ:	2020990796
IČ DPH:	SK2020990796
Bankové spojenie:	IBAN: SK2281600000003592280010
Telefón:	+421259398518

1.2 Dodávateľ:

Obchodné meno:	NTT Slovakia s. r. o.
Sídlo:	Jozefa Hagaru 9, 83151 Bratislava, Slovenská republika
IČO:	35804262
DIČ:	2020258350
IČ DPH:	SK2020258350
Bankové spojenie:	IBAN: SK5211000000002629712151
Telefón:	+421249216111

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Implementácia nového FireWall perimetra Eximbanky
Kľúčové slová:	FireWall, kybernetická bezpečnosť, VPN, konfigurácia LAN, bezpečnosť informačných systémov, bezpečnosť počítačových sietí, security gateway, CheckPoint, manažment zariadení.
CPV:	32420000-3 - Sieťové zariadenia; 30210000-4 - Stroje na spracovanie údajov (hardvér); 32422000-7 - Sieťové komponenty; 32425000-8 - Sieťový operačný systém; 48214000-1 - Softvérový balík pre sieťové operačné systémy; 48730000-4 - Softvérový balík na zaistenie bezpečnosti; 72265000-0 - Konfigurovanie softvéru; 72228000-9 - Poradenstvo pri integrácii hardvéru; 72100000-6 - Hardvérové konzultačné služby (poradenstvo); 72710000-0 - Služby pre lokálne siete LAN; 60000000-8 - Dopravné služby (bez prepravy odpadu)
Druh/y:	Tovar; Služba

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

Zoznam položiek:

1. Perimeter FW cluster
2. Interný FW – licencia cluster
3. VPN klient- licencie
4. Management bezpečnostného riešenia
5. Služby implementácie
6. Služby podpory

Položka č. 1: Perimeter FW cluster

Funkcia

Požadovaný perimeter firewall cluster s rozšírenými security funkciami je určený pre zabezpečenie perimetrovej komunikácie spoločnosti Eximbanka. pri prístupe do verejnej siete Internet a dátových sietí tretích strán.Zároveň bude slúžiť pre zabezpečenie kryptovanej komunikácie s tretími stranami formou Site-to-Site VPN tunelov a zabezpečenie vzdialeného prístupu pre minimálne 90 pracovníkov do IT infraštruktúry organizácie pomocou kryptovaného klient VPN riešenia.

Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Perimeter FW cluster	ks			1

Technické vlastnosti	**Hodnota/Charakteristika**
Perimeter firewall s rozšírenými security funkcionalitami sa skladá z dvoch zariadení v redundantnom zapojení pre zabezpečenie vysokej dostupnosti komunikačného riešenia smerom do vonkajších sietí (HA). Verejný obstarávateľ požaduje z dôvodu kompatibility s existujúcim vonkajším FireWallom Eximbanky dodávku zariadení od spoločnosti CheckPoint.	
Verejný obstarávateľ pripúšťa taktiež dodávku ekvivalentných zariadení v rovnakej alebo vyššej kvalite podľa Technickej špecifikácie predmetu zákazky kompatibilné s existujúcim vonkajším FireWallom Eximbanky špecifikovaným v položke 2. predmetného opisného formuláru.	
Každé z dodaných zariadení musí samostatne spĺňať požadované výkonové a funkčné parametre uvedené v tomto popise:Forma samostatného špecializovaného hardware zariadenia (HW Appliance),Prevedenie pre 19“ Rack, maximálna hĺbka zariadenia 510 mm,Minimálne 8ks 10/100/1000 Base-T portov pre dátovú komunikáciu,Samostatný management 10/100/1000 Base-T port a samostatný RJ45 console port,Napájací zdroj minimálne 1 x AC 230V/50Hz,Lokálny HDD, min 1x 200 GB, prevedenie SSD.	
Dodané zariadenia musia podporovať tieto komunikačné technológie a protokoly:OSPFv2 and v3, BGP, RIP, Static routes, Policy-based routing, PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3,Active/Active L2, Active/Passive L2 and L3, Session failover for routing change, device and link failure,ClusterXL, VRRP, alebo ekvivalentNAT66, NAT64, NAT46,integrácia s Microsoft AD, možnosť podpory pre LDAP a RADIUS.	
Súčasťou dodávky zariadení musí byť:HW a SW podpora výrobcu po dobu minimálne 1 roku od inštalácie zariadení (riešenia) s pokrytím 9x5 a odstránením nahlásenej závady najneskôr nasledujúci pracovný deň (NBD),Podpora a licencia na všetky požadované security funkcionality na obdobie minimálne 1 roku.Podpora a zastúpenia výrobcu na území SR z dôvodu zabezpečenia požadovaných reakčných časov.	
FW cluster riešenie musí podporovať a zabezpečovať nasledovné služby, funkcionality a nastavenia:Podpora plnej redundancie komunikačného riešenia (clustra) vytvoreného z dvoch zariadení v režime Active-Standby so stavovou synchronizáciou oboch zahrnutých zariadení,Podpora Load Share módu A-A L2,Šifrovaná cluster komunikácia,Podpora agregácie fyzických portov LACP,Podpora dual stack IPv4 a IPv6,Dostupné preddefinované threat ochrany a profily pre IPS, Antivirus, Anti-botnet a Zero-day zabezpečenie,Podpora SNI HTTPS klasifikácie a inšpekcie,Podpora ICAP serveru a ICAP clienta.	

FW cluster riešenie musí podporovať a zabezpečovať nasledovné služby, funkcionality a nastavenia (pokračovanie):Ochrana proti SNI spoofing v rámci HTTPs inšpekcie,Podpora S2S VPN, min. podpora algoritmov pre šifrovanie: AES-128, AES-256 a integritu: SHA-256 a AES-XCBC,Podpora IP kompresie pre S2S VPN,Podpora deskripcie TLS 1.3,Kontrola SMBv3 Multichannel inspection Support with AV and TE,Podpora SSH Proxy a možnosť dekripcie SSH komunikácie,Podpora RSYNC pre zálohovanie iba rozdielovej konfigurácie,Generované bezpečnostné logy sa musia ukladať na fyzicky oddelenej management platforme.	
FW cluster riešenie musí podporovať prácu s identitami:Zobrazenie užívateľskej notifikácie pri prístupe pre protokoly HTTP a HTTPS (blokácia a dotázanie užívateľa v prípade potreby),Možnosť získavania identít užívateľov z AD bez nutnosti inštalácie dodatočného software na AD servery,Zdieľanie identít medzi jednotlivými implementovanými firewallami bez nutnosti externých licencovaných komponentov.	
Min. priepustnosť/kvantitatívne parametre Firewallu:1 Gbps s rozšírenými security funkciami, vrátane možnosti Zero-Day Protection funkcionalít,Počet nových komunikačných spojení za sekundu (CPS) min. 30.000,Počet súčasných komunikačných spojení, min. 1.000.000,Možnosť detekcie, riadenia a filtrácie aplikácií - požiadavka na minimálny počet rozpoznávaných aplikácií je 5000,Detekcia a riadenie dátových súborov a typov na základe obsahu. Počet predefinovaných dátových typov min 50.	
Minimálne podporované security vlastnosti a funkcionality:Stavový L4 Firewall,podpora Site-to-Site a Client VPN,podpora pre Mobile Access riešenie,Content Awareness,Application Control,HTTPS inspection,IPS,URL Filtering,Antivirus,Antibot,Anti-Spam.	
Ďalšie požadované vlastnosti FW clustera:Možnosť vytvárania vlastných dátových typov na základe kľúčových slov, regex, súborových atribútov, vážených slov a pod.,Podpora URL filteringu na základe kategorizácie. Poskytované riešenie musí pokrývať min. 80% top milion sites (napríklad Alexa, Majestic a pod.),Integrovaný firewall performance analyzer so zobrazením minimálne top 10 spojení a ich % konzumácia HW zdrojov/pre každé spojenie/protokol.	
Vyžaduje sa , aby perimeter firewall umožňoval rozšírenie aj o security funkcionality typu SandBoxing a Zero-Day Threaths Extraction a to formou doplnenia príslušného licenčného rozšírenia riešenia bez potreby doplnenia alebo výmeny dodaných HW Appliance.	

Položka č. 2: Interný FW – licencia cluster

Funkcia				
Interný firewall umožní riadenie dátovej komunikácie medzi jednotlivými LAN segmentmi organizácie, užívateľskými LAN segmentmi a DC segmentami a taktiež medzi jednotlivými aplikáciami v lokálnom DC organizácie.Musí zároveň podporovať v prípade potreby aj nasadenie funkcionality IDS (Intrusion Detection System), ktorá umožní bezpečnostné skenovanie prebiehajúcej internej dátovej komunikácie na základe security signatúr s cieľom detekcie nežiadúcich malware aktivít na požadovaných segmentoch internej komunikačnej infraštruktúry organizácie.				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Interný FW – licencia cluster	ks			1
Technické vlastnosti	**Hodnota/Charakteristika**			

Interný sieťový firewall bude migrovaný z existujúceho FW riešenia Eximbanky, 2 ks zariadenia Checkpoint UTM modelového radu 3200 (SN: 1715BA0651 a 1715BA0658). Zariadenia majú platnú apliance do 8.6.2023, verejný obstarávateľ požaduje predĺženie subskripcie pre licencie a podporu zariadení na ďalší rok. Vyžaduje sa podpora a zastúpenie výrobcu na území SR z dôvodu zabezpečenia požadovaných reakčných časov.Je požadovaná podpora plnej redundancie komunikačného riešenia (clustra) vytvoreného z dvoch zariadení v režime Active-Standby so stavovou synchronizáciou oboch zahrnutých zariadení.	
Riešenie interného FW clustera musí podporovať a zabezpečovať nasledovné služby, funkcionality a nastavenia:Podpora Load Share módu A-A L2,Šifrovaná cluster komunikácia,Podpora agregácie fyzických portov LACP,Podpora dual stack IPv4 a IPv6,Dostupné preddefinované threat ochrany a profily pre IPS, Antivirus, Anti-botnet a Zero-day zabezpečenie,Podpora SNI HTTPS klasifikácie a inšpekcieBlokácia SQL Injection a CSS útokov v URL a HTML body,Podpora detekcie a riadenia sieťových aplikácií/pluginov pre sociálne siete,Podpora explicitnej HTTP/HTTPS proxy,Podpora ICAP serveru a ICAP klienta.	
Riešenie interného FW clustera musí podporovať a zabezpečovať nasledovné služby, funkcionality a nastavenia (pokračovanie):Ochrana proti SNI spoofing v rámci HTTPs inšpekcie,Podpora deskripcie TLS 1.3,Kontrola SMBv3 Multichannel inspection Support with AV and TE,Podpora SSH Proxy a možnosť dekripcie SSH komunikácie,Podpora RSYNC pre zálohovanie iba rozdielovej konfigurácie,Generované bezpečnostné logy sa musia ukladať na fyzicky oddelenej management platforme	
FW cluster riešenie musí podporovať prácu z identitami:Zobrazenie užívateľskej notifikácie pri prístupe pre protokoly HTTP a HTTPS (blokácia a dotázanie užívateľa v prípade potreby),Možnosť získavania identít užívateľov z AD bez nutnosti inštalácie dodatočného software na AD servery,Zdieľanie identít medzi jednotlivými implementovanými firewallami bez nutnosti externých licencovaných komponentov.	

Položka č. 3: VPN klient- licencie

Funkcia				
Požadovaný SW security klient inštalovaný na koncových užívateľských zariadeniach, PC a/alebo notebookoch, mobilných zariadení typu tablet/mobilný telefón zamestnancov spoločnosti Eximbanky bude využívaný pre zriadenie bezpečného vzdialeného dátového pripojenia zamestnancov do IT infraštruktúry verejného obstarávateľa pomocou kryptovaného klienta VPN prístupu s využitím perimeter FW clustra.				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
VPN klient- licencie	ks			90
Technické vlastnosti	**Hodnota/Charakteristika**			
VPN klient musí podporovať minimálne tieto operačné systémy:Microsoft Windows 8 a vyššie,Microsoft Windows Server 2016 a vyššie,Mac OS 11.00 a vyššie,IOS 15 a vyššie,Android 11 a vyššie.				

Pre účely dátového zabezpečenia koncového zariadenia musí VPN klient podporovať minimálne tieto funkcionality:Remote Access VPN,DLP,Antivírová ochrana,Používanie logických užívateľských skupín koncových užívateľov,Integrácia so službou MS Active Directory,Možnosť definovania administrátorských rolí,Podpora VPN funkcionality aj prostredí s NAT a security zariadeniami, ktoré nepodporujú IPSec prevádzku (napríklad podpora tunelingu VPN cez HTTPS).	
Modulárna architektúra, ktorá umožní aktiváciu jednotlivých komponentov zabezpečenia koncového zariadenia takým spôsobom, aby mohlo byť v prípade potreby kombinované s existujúcimi, prípadne inými v budúcnosti požadovanými bezpečnostnými riešeniami tretích strán implementovanými na koncových zariadeniach,	
Požiadavky pre bezpečnostné politiky:Správa bezpečnostných politík pre koncové zriadenia je požadovaná na úrovni konkrétneho užívateľa a/alebo skupiny užívateľov,Bezpečnostné politiky a citlivé informácie prenášané medzi manažment serverom riešenia a koncovým užívateľským zariadením musia byť počas prenosu šifrované,Podpora centrálnej správy bezpečnostných pravidiel a práce s logmi,Podpora konfigurácie bezpečnostných politík aj prostredníctvom lokálneho GUI rozhrania, ku ktorému je možné sa pripojiť aj pomocou šifrovaného protokolu.	
Koncoví užívateľa ani v prípade, ak majú pridelené práva lokálneho administrátora koncového zariadenia nemôžu- mať možnosť ovládať, alebo meniť konfiguračné parametre koncového zariadenia a to ani v prípade, ak má užívateľ pridelené oprávnenie ako lokálny administrátora zariadenia,- mať možnosť obísť bezpečnostné pravidlá implementované v rámci data security zabezpečenia koncového zariadenia,- odinštalovať SW security agenta zo zariadenia,- zastaviť alebo iným spôsobom ovplyvňovať funkcionalitu security agenta na koncovom zariadení.	
Požiadavky na bezpečnostný SW/klienta koncového zariadenia:Bezpečnostný software alebo agenti nainštalovaní na koncových užívateľských zariadeniach nevyžadujú lokálne administrátorské práva pre spustenie alebo aktualizáciu,Security klient koncového zariadenia musí mať integrovanú funkcionalitu IPSec VPN,Security klient koncového zariadenia musí podporovať takzvaný "Split Tunnelling", t.j. možnosť prístupu k povoleným internetovým portálom aj mimo VPN tunela, ale intranetová komunikácia organizácie je smerovaná do vytvoreného šifrovaného tunela.	
Požiadavky na overovanie koncových užívateľov:Overovanie koncových užívateľov pri VPN prístupe na perimeter firewall musí podporovať využívanie užívateľského mena/hesla alebo klientského certifikátu,Podpora multifaktorovej autentifikácie. Možnosť integrácie s riešením jednorazového hesla (OTP) ako doplnok k užívateľskému heslu (dvojfaktorová autentifikácia), napríklad vo forme SMS správy, aplikácie na mobilnom telefóne a pod.,V rámci centrálneho managementu podpora funkcionality Internej CA (Certifikačnej autority) pre správu užívateľských certifikátov pre VPN autentifikáciu endpointov.	
Podpora funkcionality korelácie logov, analýzy a správy bezpečnostných udalostí s predefinovanými šablónami a reportmi, vrátane previazanosti s logmi s network a perimeter firewallmi.	

Položka č. 4: Management bezpečnostného riešenia

Funkcia				
Manažmentom riešenia sa myslí nástroj na správu oboch Firewall Clustrov a Endpoint security riešenia, ktorý plní tieto funkcie:Manažment a konfiguračná správa perimeter firewall clustra s rozšírenými security funkcionalitami,Manažment a konfiguračná správa interného segmentačného LAN/DC firewall clustra,Manažment a konfiguračná správa endpoint security riešenia pre približne 200 koncových zariadení zamestnancov spoločnosti Eximbanka a S2S VPN.				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Management bezpečnostného riešenia	ks			1
Technické vlastnosti	**Hodnota/Charakteristika**			
Vyžaduje sa využiť existujúci jednotný management riešenia aj pre nový perimeter FW cluster a nové VPN pripojenia a v prípade potreby aj upgrade alebo update súčasného managementu. Alternatívou je vytvoriť nové management riešenie pre všetky zariadenia vo forme SW aplikácie na inštalovanej na virtuálny server verejného obstarávateľa.Predmetom dodávky musia byť aj všetky licencie potrebné na prevádzku takéhoto riešenia.Je požadovaná licenčná podpora pre všetky zariadenia Perimeter Firewall, Interný FW a užívateľov security VPN klient.				
Management musí zabezpečiť spracovávanie a archiváciu logov zo všetkých firewallov a koncových užívateľských zariadení s inštalovaným security a VPN klientom navrhovaného výrobcu v IT infraštruktúre verejného obstarávateľa. Je potrebné rátať s objemom logov minimálne 500MB/deň a dodané riešenie musí mať schopnosť spracovať min. 1 000 logov/sekundu.Management musí byť schopný dohľadať pre každý objekt, jeho výskyt v aktívnych aj neaktívnych pravidlách, alebo v iných objektoch (napr. v objektových skupinách).				
Požiadavky pre bezpečnostné politiky:Jednotný management dátových bezpečnostných politík cez GUI prostredie, analýza logov a reporting v rámci jednotného konsolidovaného manažmentu pre koncové užívateľské zariadenia, perimeter firewallu a interného FW, na ktorom budú ukončované klientské VPN prístupy,Možnosť integrácie na VMware vSphere a Vmware NSX, min. dynamické získavanie VM objektov a ich aplikácia vo firewall politikách,Možnosť segmentácie politík do samostatných logických oddielov, zoskupovanie firewall pravidiel do logických skupín na základe zdroja, cieľa, služby/aplikácie.				
Požiadavky pre bezpečnostné politiky (pokračovanie):Kontrola politik proti chybám a duplicitám, Policy TracerVizualizácia a analýza logov priamo v politike na vybranom pravidle (min. zdroj, cieľ, služba, aplikácia, používateľ, čas),Zobrazenie histórie a zmien priamo v politike na vybranom pravidle (min. kto, aká zmena a kedy bola na pravidle vykonaná),Podpora tvorby revízií jednotlivých verzií bezpečnostnej politiky,Hit count štatistiky pre jednotlivé pravidlá s cieľom optimalizácie bezpečnostnej politiky.				
Požiadavky na možnosti administrátorských profilov:Podpora administrátorských profilov pre delegáciu oprávnení (čítanie, zápis),Možnosť pridelenia práv administrátorom alebo API účtu iba pre definovaný zoznam prístupových firewall pravidiel,Ochrana vzájomného ovplyvňovania alebo kolízie pri súčasnom pripojení viacerých administrátorov (zamykanie pravidiel a objektov).				

Požiadavky na prácu s logmi:Funkcionalita filtrácie logov a analýzy s predefinovanými pohľadmi a filtrami,Prehľadávanie logov, min. podpora: "keyword" prehľadávanie, "field" prehľadávanie a "wildcard" prehľadávaná,Práca s bezpečnostnými logmi - možnosť prehľadávania všetkých typov logov (fw, ips, malware) v jednej záložke s definovaním vlastných filtrov,Podpora korelácie bezpečnostných logov a incidentov,Tvorba vlastných definícií log parserov.	
Požiadavky na reporting a monitoring dodaného riešenia:Musí podporovať nástroj pre definíciu šablón pre generovanie reportov,Musí graficky zobrazovať jednotlivé kategórie udalostí vo forme prehľadných interaktívnych koláčových a časových grafov,Musí poskytovať grafické rozhranie pre sledovanie parametrov v reálnom čase a histórii aspoň 30 dní (využitie pamäte, CPU, počet naviazaných spojení, počet novo-otvorených spojení za sekundu, priepustnosť, atď ...).	
Ďalšie požiadavky:Kontrola bezpečnostných politík podľa štandardov, min. napríklad ISO 27000 a GDRP,Podpora pravidelného automatického zálohovania konfigurácie (na základe časového rozvrhu), s možnosťou nahrania zálohy na vzdialený server,Podpora služby vlastnej certifikačnej autority pre vydávanie PKI certifikátov pre bezpečné prihlasovanie užívateľov a administrátorov a pre VPN klientsky prístup,Integrácia SAML 2.0 autentizačných služieb pre overovanie a získavanie identít užívateľov.	

Položka č. 5: Služby implementácie

Funkcia				
Ako súčasť dodávky bezpečnostného riešenia požaduje verejný obstarávateľ dodať služby v súlade s technickou špecifikáciou, ktoré sú uvedené v technických vlastnostiach pre túto položku. Miestom dodávky služieb je sídlo verejného obstarávateľa.				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Služby implementácie	ks			1
Technické vlastnosti	**Hodnota/Charakteristika**			
Analýza aktuálneho riešenia infraštruktúry verejného obstarávateľa, návrh nového sieťového dizajnu pre implementáciu bezpečnostného riešenia (LLD dizajn).				
Spracovanie projektového plánu a časového harmonogramu pre implementáciu riešenia v IT infraštruktúre verejného obstarávateľa v súlade s navrhovaným a odsúhlaseným LLD dizajnom.				
Rekonfigurácia existujúcej IT infraštruktúry (WAN/LAN/DC/...) verejného obstarávateľa pre účely implementácie nového bezpečnostného riešenia v súlade s odsúhlaseným LLD dizajnom.				
Spolupráca s poskytovateľom internetovej konektivity pri nastavení WAN pripojenia.				
HW a SW inštalácia bezpečnostného riešenia v IT infraštruktúre verejného obstarávateľa vrátane aktualizácie HW a SW riešenia používaného v súčasnosti v EXIMBANKA SR.				
Migrácia exitujúcich základných perimeter routing a FW politík na nové bezpečnostné riešenie.				
Aktivácia a konfigurácia rozšírených security funkcionalít obsiahnutých v rámci bezpečnostného riešenia v súlade s navrhnutým a odsúhlaseným LLD dizajnom.				
Implementácia a registrácia zariadení pod správu konsolidovaného management servera v IT infraštruktúre verejného obstarávateľa.				

Overenie správnej funkčnosti dátovej komunikácie v IT infraštruktúre verejného obstarávateľa v súlade s odsúhlaseným LLD dizajnom.	
Príprava typového SW balíku pre inštaláciu a nasadenie navrhovaného SW endpoint security riešenia na koncových zariadeniach spoločnosti Eximbanka.	
Realizácia typovej inštalácie navrhovaného SW endpoint security klienta na max. troch endpoint zariadeniach.	
Implementácia a registrácia SW endpoint security riešenia pod správu management servera v IT infraštruktúre verejného obstarávateľa.	
SW inštalácia konsolidovaného managementu na virtuálny server v IT infraštruktúre verejného obstarávateľa.	
SW implementácia a konfigurácia konsolidovaného managementu pre správu firewall clustrov a endpoint security riešenia v súlade s požiadavkami verejného obstarávateľa.	
Overenie požadovanej funkcionality implementovaného konsolidovaného managementu v súlade s požiadavkami verejného obstarávateľa.	
Odovzdanie bezpečnostného riešenia do riadnej prevádzky verejného obstarávateľovi.	
Spracovanie technickej dokumentácie implementovaného riešenia.	
Školenie pre minimálne 2 administrátorov systému.	
Projektový management, dopravné a logistické náklady.	

Položka č. 6: Služby podpory

Funkcia				
Ako súčasť dodávky bezpečnostného riešenia požaduje verejný obstarávateľ poskytnutie služieb podpory počas obdobia 12 mesiacov odo dňa dodávky HW a SW komponentov bezpečnostného riešenia, ktoré sú uvedené v technických vlastnostiach pre túto položku. Miestom dodávky služieb je sídlo verejného obstarávateľa.				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Služby podpory	MD		12	
Technické vlastnosti	**Hodnota/Charakteristika**			
Licencie funkcionalít pre zariadenia perimeter firewall				
Licencie funkcionalít pre zariadenia interný FW.				
Licencie funkcionalít pre security VPN klient (pre všetkých užívateľov).				
Licencie funkcionalít pre management.				
Formou rámcového kontraktu 12 človekodní, ktoré si Verejný obstarávateľ vyhradzuje čerpať na základe jeho aktuálnych potrieb nad rámec služieb popísaných ako služby implementácie počas platnosti trvania zmluvy, vždy na základe konkrétnej čiastkovej objednávky. Uvedený rozsah Služieb podpory sa stane záväzný po potvrdení objednávky zo strany objednávateľa. Čerpanie uvedeného rozsahu nie je nárokovateľné zo strany dodávateľa.				

2.3 Osobitné požiadavky na plnenie:

Názov
Vrátane dopravy na miesto plnenia , ktorým je adresa sídla objednávateľa, priamo zodpovednej osobe objednávateľa (podrobnosti o mieste plnenia a zodpovednej osobe objednávateľa budú dodávateľovi oznámené bezodkladne po nadobudnutí účinnosti zmluvy).

Ak sa v opisnom formulári uvádzajú údaje alebo odkazy na konkrétneho výrobcu, výrobný postup, značku, obchodný názov, patent alebo typ, umožňuje sa dodávateľovi predloženie ponuky s ekvivalentným riešením s porovnateľnými, respektíve lepšími parametrami. Ekvivalent je možné dodať v rovnakej alebo vyššej kvalite podľa Technickej špecifikácie predmetu zákazky.
Požaduje sa dodanie podľa nasledovného harmonogramu:Perimeter FW cluster- dodávka HW zariadení a licencií do 10-týždňov po nadobudnutí účinnosti zmluvy,Interný FW – obnova licencií pre existujúce cluster zariadenia spoločne s Manažment licenciami a licencie VPN klient- do 5 pracovných dní po nadobudnutí účinnosti zmluvy,Služby implementácie- do 12 týždňov dodávky HW zariadení podľa bodu 1,Služby podpory- počas obdobia 12 mesiacov po odovzdaní celého riešenia.
Pre všetky dodávky platí nasledovné:- na dohodnuté miesto plnenia,- v pracovný deň od 9 00 do 15 00,- s dodacím listom/akceptačným protokolom, ktorý musí obsahovať okrem povinných náležitostí číslo zmluvy, jednotkovú cenu bez DPH, jednotkovú cenu s DPH, sadzbu DPH, celkovú cenu bez DPH a celkovú cenu s DPH.
Po podpísaní akceptačného protokolu na ktorúkoľvek časť plnenia zakladá dodávateľovi právo na vystavenie faktúry. Splatnosť faktúry je 30 dní.
Dodávateľ je povinný dodať všetky položky predmetu zákazky nové, nepoužívané, nerepasované a v neporušenom originálnom balení ako celok.
Dodávateľ vyhlasuje, že dodá predmet zákazky, ktorý je certifikovaný a schválený na dovoz a predaj v Slovenskej republike, resp. v rámci Európskej únie a bude vyhovovať platným medzinárodným normám, STN a všeobecne záväzným právnym predpisom.
Dodávateľ vyhlasuje, že predmet plnenia (najmä, no nie výlučne poskytovanie služieb podľa bodov 5. a 6.) bude poskytovať odborne spôsobilá osoba , ktorá disponuje certifikátom výrobcu ponúkaných zariadení, ktorý preukazuje jej odborné znalosti pre návrh a implementáciu bezpečnostných riešení v požadovanej úrovni. Dodávateľ vyhlasuje, že do troch pracovných dní od účinnosti zmluvy predloží objednávateľovi scan certifikátu výrobcu ponúkaných zariadení, ktorý preukazuje jej odborné znalosti pre návrh a implementáciu bezpečnostných riešení v požadovanej úrovni.
Dodávateľ vyhlasuje, že disponuje certifikátom , ktorý bol vydaný výrobcom ponúkaných zariadení o jeho oprávnení, schopnosti dodávať uvedený tovar a poskytovať súvisiace služby (napríklad partnerský certifikát, alebo iný ekvivalent). Dodávateľ vyhlasuje, že do troch pracovných dní od účinnosti zmluvy predloží objednávateľovi scan certifikátu , ktorý bol vydaný výrobcom ponúkaných zariadení o jeho oprávnení, schopnosti dodávať uvedený tovar a poskytovať súvisiace služby (napríklad partnerský certifikát, alebo iný ekvivalent).
Ak sa ktorékoľvek z vyhlásení dodávateľa ukáže ako nepravdivé, objednávateľ má nárok odstúpiť od zmluvy.
Do troch pracovných dní od účinnosti zmluvy predloží dodávateľ verejnému obstarávateľovi:Detailnú špecifikáciu konkrétnych zariadení a licencií, ktoré chce dodať v rozsahu, ktorý umožní overiť ich súlad s technickou špecifikáciou predmetu zákazky,Certifikát, že je oprávnený dodávať predmetné zariadenia,Meno zodpovednej osoby/experta, ktorý bude realizovať zákazku aj s certifikátom výrobcu dodávaných zariadení preukazujúcim jej odborné znalosti,Detailný návrh harmonogramu na oddanie celého riešenia a implementačných prác (položky 1-5 opisného formulára).
Nedodržanie ktorejkoľvek podmienky a požiadavky objednávateľa uvedenej v objednávkovom, resp. opisnom formulári sa bude považovať za podstatné porušenie zmluvných podmienok.

Názov	Upresnenie

2.4 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát:	Slovenská republika
Kraj:	Bratislavský
Okres:	Bratislava I
Obec:	Bratislava - mestská časť Staré Mesto
Ulica:	Grösslingová 1

3.2 Čas / lehota plnenia zmluvy:

19.06.2023 09:00:00 - 31.10.2023 15:00:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka: viď jednotlivé položky opisného formulára

Požadované množstvo: 1,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronickej platformy verzia 1.2, účinná odo dňa 3.11.2022 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 100 350,00 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 120 420,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronickej platformy uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv Trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:
Príloha č.1 Obchodné podmienky elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 12.06.2023 13:38:01

Objednávateľ:
Exportno-importná banka Slovenskej republiky, skrátene EXIMBANKA SR
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
NTT Slovakia s. r. o.
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska