Příloha č. 1 ZD Čj 1/120/1702770–2019

**Podrobná specifikace dodávky HW komponent a služeb**

**+ tabulka pro tvorbu nabídkové ceny**.

Obměna firewalu, oddělení serverové a uživatelské LAN

Obsah

[**1.** **Předmět veřejné zakázky** 3](#_Toc15370930)

[**2.** **Obecné požadavky na externí a interní firewall** 3](#_Toc15370931)

[2.1 Externí firewall 3](#_Toc15370932)

[2.1.1 Základní technické požadavky 3](#_Toc15370933)

[2.1.2 Funkce detekce aplikací na L7 (Application Control) 4](#_Toc15370934)

[2.1.3 Funkce detekce a potlačení narušení (IPS/IDS) 4](#_Toc15370935)

[2.1.4 Funkce antivirové kontroly 4](#_Toc15370936)

[2.1.5 Funkce IPsec VPN 5](#_Toc15370937)

[2.1.6 Funkce SSL VPN 5](#_Toc15370938)

[2.1.7 Funkce kategorizace webových stránek 5](#_Toc15370939)

[2.1.8 Funkce DNS filtru 5](#_Toc15370940)

[2.1.9 Funkce před únikem citlivých informací (DLP) 5](#_Toc15370941)

[2.1.10 Explicit proxy 6](#_Toc15370942)

[2.1.11 Virtualizace 6](#_Toc15370943)

[2.1.12 Management 6](#_Toc15370944)

[2.1.13 Ochrana koncových stanic 6](#_Toc15370945)

[2.2 Interní firewall 7](#_Toc15370946)

[2.2.1 Základní technické požadavky 7](#_Toc15370947)

[2.2.2 Funkce detekce aplikací na L7 (Application Control) 8](#_Toc15370948)

[2.2.3 Funkce detekce a potlačení narušení (IPS/IDS) 8](#_Toc15370949)

[2.2.4 Virtualizace 8](#_Toc15370950)

[2.2.5 Management 9](#_Toc15370951)

[2.3 Zpracování logů a reporting 9](#_Toc15370952)

[**3.** **Definice služeb** 9](#_Toc15370953)

[3.1 Implementační plán 10](#_Toc15370954)

[3.2 Měsíční služby 10](#_Toc15370955)

[3.3 Školení 10](#_Toc15370956)

[**4.** **Další požadavky zadavatele** 10](#_Toc15370957)

[**5.** **Cena** 11](#_Toc15370958)

# **Předmět veřejné zakázky**

Předmětem VZ náhrada internetového firewallu (externí firewall) provozovaného na dvou Cisco ASA5515-X a doplnění LAN infrastruktury VoZP ČR dalším firewallem pro oddělení serverové a uživatelské infrastruktury (interní firewall). Externí firewall bude realizován jako pronájem na dobu 48 měsíců, interní firewall bude realizován nákupem zařízení.

V rámci této veřejné zakázky zadavatel požaduje zpracování implementačního plánu, instalaci a oživení HW, případný upgrade FW na poslední verzi, konfiguraci podle zpracovaného implementačního plánu a zpracování finální dokumentace.

Zadavatel dále požaduje, aby součástí této veřejné zakázky bylo také školení „Základní seznámení, instalace a konfigurace dodaných zařízení“.

# **Obecné požadavky na externí** **a interní firewall**

Externí firewall bude řešen jako dva samostatné stejné boxy zapojené v režimu active/active nebo active/standby. Stejně tak interní firewall bude řešen jako dva samostané stejné boxy zapojené v režimu active/active nebo active/standby.

Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 4 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. Požadujeme, aby support výrobce byl v režimu 24x7x365. Tento support bude zahrnovat HW a FW zařízení (výměna v případě nefunkčnosti zařízení nebo nových funkcionalit, které může zadavatel využít).

Externí a interní firewall musí být od stejného výrobce.

* 1. Externí firewall

Certifikace ICSA Labs minimálně pro Firewall, IPSec VPN, IPS, Antivirus, SSL VPN

* + 1. Základní technické požadavky
* HW appliance NGFW/UTM firewallu v režimu vysoké dostupnosti (dvě fyzická zařízení stejného typu zapojená do funkčního clusteru)
* Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti maximálně 1RU
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Požadujeme možnost doplnit druhý napájecí zdroj (interní nebo externí), nebo zařízení vybavené dvěma zdroji
* Min. 16x 1 GE SFP rozhraní na každém firewallu využitelných pro zpracování komunikace
* Min. 16x 1 GE RJ45 rozhraní na každém firewallu využitelných pro zpracování komunikace
* 2 x samostatné 1GE rozhraní využitelné pro management
* konzolový port pro management
* Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres; celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P)
	+ Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky
* Možnost rozšíření režimu vysoké dostupnosti na až 4 členy clusteru (včetně podpory režimu A-A) resp dva samostatné clustery o dvou zařízeních (budoucí topologie není v tuto chvíli přesně dána).

Požadované síťové a bezpečnostní funkce, součástí dodávky musí být i příslušná licence (je-li výrobcem požadována) na 4 roky. Požadované výkonnostní parametry musí být oficiálně deklarovány výrobcem firewallu.

* Podpora VLAN (až 4000)
* Podpora LACP
* Počet FW pravidel až 10.000
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Celková propustnost firewall min. 32/32/20 Gbps (měřeno na UDP paketech o velikosti 1518B/512B/64B)
* Vložená latence firewallu nepřesahuje 4 µs (měřeno na malých UDP paketech (64B))
* Počet nově navázaných TCP spojení (setup-rate) min. 280.000 za sekundu
* Celkový počet konkuretních TCP spojení firewallu 4 miliony
* PPS (počet zpracovaných paketů za 1 sekundu) min. 30M
	+ 1. Funkce detekce aplikací na L7 (Application Control)
	+ Detekce známých aplikací na základě signatur
	+ Signaturový database automaticky aktualizované výrobcem
	+ alespoň 4000 podporovaných aplikací
	+ pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé fakce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
	+ možnost tvorby vlastních signatur
	+ detekované aplikace je možné: povolit, monitorovat, blokovat
	+ na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
	+ funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
		1. Funkce detekce a potlačení narušení (IPS/IDS)
	+ signatury automaticky aktualizované výrobcem
	+ alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
	+ možnost tvorby vlastních signatur
	+ funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
	+ propustnost funkce IPS včetně logování min. 5Gbps (měřeno na komunikaci typu mix aplikací)
		1. Funkce antivirové kontroly
	+ Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem
	+ signatury automaticky aktualizované výrobcem
	+ požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
	+ možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce
	+ deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 3Gbps
	+ funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
	+ Podpora služby výrobce, které umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
	+ Funkce odstranění́ aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu. Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
	+ Podpora SSL dekrypce/SSL inspekce s minimální propustností 3,5Gbps
	+ Minimální množství současně navázaných session s SSL inspekcí: 300 000
		1. Funkce IPsec VPN
	+ podpora site-to-site VPN
	+ podpora klientských VPN
	+ dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
	+ funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence.
	+ Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 2.000
	+ Minimální počet klientských IPSEC VPN tunelů: 40.000
	+ propustnost IPSec VPN min. 20 Gbps (měřeno při AES 256-SHA 256)
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
	+ podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
		1. Funkce SSL VPN
	+ Podpora klientského i bezklientského (portálového) režimu
	+ Minimální počet současně navázaných SSL VPN tunelů: 400
	+ Minimální propustnost SSL VPN: 2,5Gbps
		1. Funkce kategorizace webových stránek
	+ založená na centrálně spravované databázi výrobce
	+ minimálně 50 filtračních kategorií
	+ možnost definice vlastních kategorií
	+ možnost definice vlastních seznamů zakázaných URL
	+ kategorizace musí zahrnovat I české a slovenské internetové stránky
		1. Funkce DNS filtru
	+ Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
	+ Možnost definovat vlastní tzv. blacklist domén
	+ Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
	+ Možnost importu seznamu blokovaných domén do DNS filtru
		1. Funkce před únikem citlivých informací (DLP)
	+ možností analýzy běžných typů dokumentů a protokolů
	+ možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum
		1. Explicit proxy
	+ podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
	+ podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
	+ funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
	+ Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru
		1. Virtualizace
	+ Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální context musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
	+ Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
	+ Každý virtuální context je zároveň samostatným wifi kontrolérem
	+ Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)
		1. Management
* FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* Požadujeme jediné management rozhraní pro celý cluster, změna konfigurace je mezi jednotlivými členy clusteru synchronizována automaticky
* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)
* Podpora vazby na Cisco Identity Services Engine (ISE)
	+ 1. Ochrana koncových stanic

Požadujeme dodání softwaru pro ochranu koncových stanic, který bude zajišťovat tyto funkce:

* Možnost navázání IPsec VPN nebo SSL VPN na dodávanou bezpečnostní bránu (firewall)
* Možnost vytvoření instalačního msi balíčku s předkonfigurovanými parametry
* Možnost modulární instalace klienta
* Dostupnost klienta minimálně pro tyto operační systémy: Windows, macOS, Linux, Android, iOS
* Integrace s poptávanou bezpečnostní bránou ve smyslu předávání informace o klientovi do sítě, možnost karantény až na úrovni koncového prvku, informace o odhalených zranitelnostech na koncových stanicích
* Možnost vynucení bezpečnostních politik kde, když je koncový prvek nebude splňovat, tak zobrazení varovné hlášky anebo zablokování přístupu do sítě
* Pokud se jedná o licencovanou funkcionalitu, tak požadujeme licence pro současně 100 připojených klientů po dobu 4 let
* Možnost rozdílného nastavení klientů, když jsou v interní síti a mimo interní síť
* Antivirovou ochranu koncových stanice včetně automatické kontroly vyměnitelných médií
* Ochranu uživatelů před přístupem na škodlivé webové stránky
* Možnost centrální správy koncových softwaru pro ochranu koncových stanic
* Centrální správa by měla obsahovat tyto funkce:
	+ Možnost aplikace různých profilů s nastavením na různé skupiny ve Windows AD
	+ Zajištění automatické instalace v rámci Windows domény
	+ Dohled nad všemi klienty
	+ Možnost vynucení kontroly zranitelností anebo kontroly na přítomnost malware v koncové stanici
	+ Výpis nainstalovaných aplikací na koncové stanici a upozornění na případné zranitelnosti
	+ Možnost vložit koncovou stanici do karantény
	+ Možnost vzdáleně provést upgrade klienta
	+ Možnost odinstalovat klienta z koncové stanice
	+ Možnost přihlášení administrátora do systému centrální správy s ověřením na LDAP
	+ Pokud se jedná o licencované řešení, tak požadujeme licenci pro 100 koncových zařízení pod dobu 4 let
	1. Interní firewall
		1. Základní technické požadavky
* HW appliance NGFW/UTM firewallu v režimu vysoké dostupnosti (dvě fyzická zařízení stejného typu zapojená do funkčního clusteru)
* Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti maximálně 2RU
* Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu
* Požadujeme možnost doplnit druhý napájecí zdroj (interní nebo externí), nebo zařízení vybavené dvěma zdroji
* Min. 8x 1 GE SFP rozhraní na každém firewallu využitelných pro zpracování komunikace, HW akcelerované
* Min. 16x 1 GE RJ45 rozhraní na každém firewallu využitelných pro zpracování komunikace, HW akcelerované
* Min. 4x 10GE SFP+ rozhraní na každém firewallu využitelných pro zpracování komunikace, HW akcelerované
* Min. 4x 25GE SFP28/10GE SFP+ rozhraní na každém firewallu využitelných pro zpracování komunikace, HW akcelerované
* Min. 2x 40GE QSFP+ rozhraní na každém firewallu využitelných pro zpracování komunikace, HW akcelerované
* 2 x samostatné 1GE rozhraní využitelné pro management
* konzolový port pro management
* Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres; celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P)
* Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky
* Možnost rozšíření režimu vysoké dostupnosti na až 4 členy clusteru (včetně podpory režimu A-A) resp dva samostatné clustery o dvou zařízeních (budoucí topologie není v tuto chvíli přesně dána).
* Integrovaný disk (nebo disky) celkové kapacity min 1x480GB pro lokální ukládání logů v případě výpadku centrálního log serveru

Požadované síťové a bezpečnostní funkce, součástí dodávky musí být i příslušná licence (je-li výrobcem požadována) na 4 roky. Požadované výkonnostní parametry musí být oficiálně deklarovány výrobcem firewallu.

* Podpora VLAN (až 4000)
* Podpora LACP
* Počet FW pravidel až 90.000
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Celková propustnost firewall min. 80/80/50 Gbps (měřeno na UDP paketech o velikosti 1518B/512B/64B)
* Vložená latence firewallu nepřesahuje 4 µs (měřeno na malých UDP paketech (64B))
* Počet nově navázaných TCP spojení (setup-rate) min. 280.000 za sekundu
* Celkový počet konkuretních TCP spojení firewallu 11 milionu
* PPS (počet zpracovaných paketů za 1 sekundu) min. 80M
	+ 1. Funkce detekce aplikací na L7 (Application Control)
	+ Detekce známých aplikací na základě signatur
	+ Signaturový database automaticky aktualizované výrobcem
	+ alespoň 4000 podporovaných aplikací
	+ pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé fakce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
	+ možnost tvorby vlastních signatur
	+ detekované aplikace je možné: povolit, monitorovat, blokovat
	+ na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
	+ funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
		1. Funkce detekce a potlačení narušení (IPS/IDS)
	+ signatury automaticky aktualizované výrobcem
	+ alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
	+ možnost tvorby vlastních signatur
	+ funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
	+ propustnost funkce IPS včetně logování min. 12Gbps (měřeno na komunikaci typu mix aplikací)
		1. Virtualizace
	+ Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální context musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
	+ Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
	+ Každý virtuální context je zároveň samostatným wifi kontrolérem
	+ Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)
		1. Management
* FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* Požadujeme jediné management rozhraní pro celý cluster, změna konfigurace je mezi jednotlivými členy clusteru synchronizována automaticky
* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)
* Podpora vazby na Cisco Identity Services Engine (ISE)
	1. Zpracování logů a reporting

Požadujeme samostané řešení pro zpracování logů a reporting

* + Logovací/reportovací nástroj musí být od stejného výrobce, jako je FW řešení
	+ Požadujeme plnou integraci s FW řešením, včetně obousměrné komunikace (tj. logy uložené na logserveru musí být možné prohlížet přímo z MGMT rozhraní firewallu)
	+ Možnost detailního prohledávání logů
	+ Přehled aktuálního stavu FW clusteru a událostí formou widgetů s podporou funkce DrillDown
		- Cílem je rychle identifikovat případný problém v síti (síťový, bezpečnostní, …)
		- včetně přehledu stavu wifi infrastruktury (počet wifi klientů, neautorizované AP atp.)
* Široká nabídka předpřipravených reportů (nejčastěji využívaných reportů- bezpečnostní incidenty, využití konektivity, navštěvované kategorie stránek, atd.)
* Možnost tvorby vlastních detailních reportů
* Možnost exportu reportů (HTML, PDF, CSV, XML)
* Podpora vyhodnocování událostí a upozornění na ně (email, snmp trap)
	+ - Možnost vlastní definice monitorovaných událostí
	+ Forma VM appliance pro platformu VMWare ESX/Hyper-V
	+ Podpora multi-tenantního prostředí (tj. oddělené rozhraní na log/reporting
	+ Požadujeme podporu pro ukládání logů až 3TB
	+ Denní objem přijatých logů min. 6GB
	+ S přihlédnutím na další rozvoj řešení požadujeme možnost sbírat logy až z 10 firewallů.

# **Definice služeb**

Dodavatel zajistí časovou návaznost jednotlivých činností (instalace, konfigurace, testování, provoz) tak, aby nedošlo k omezení provozu VoZP ČR. Zadavatel požaduje vypracování celkového časového harmonogramu provádění jednotlivých činností (Implementační plán).

* 1. Implementační plán

Návrh implementačního plánu:

|  |  |  |
| --- | --- | --- |
| Čas (T + týden) | Činnost | Poznámka |
| 1 | Zpracování implementačního plánu |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 | Instalace zařízení |  |
| 6 |  |
| 7 | Konfigurace zařízení |  |
| 8 |  |
| 9 |  |
| 10 |  |
| 11 | Testovací provoz |  |
| 12 |  |
| 13 | Finální úpravy konfigurace |  |
| 14 | Rutinní provoz se zvýšeným dohledem |  |
| 15 | Odpojení ASA5515 |
| 16 | Vypracování dokumentace |  |

T = datum účinnosti smlouvy

Dodavatel může navrhovanou tabulku implementačního plánu změnit podle svého uvážení a zkušeností, nicméně celková doba implementace 16 týdnů nesmí být překročena, taktéž musí být zachována doba testovacího provozu a rutinního provozu se zvýšeným dohledem (2 týdny)

* 1. Měsíční služby

Zadavatel požaduje dodání externího firewallu jako službu s měsíční platbou na dobu 48 měsíců. Během doby 48 měsíců zadavatel nepředpokládá zásadní změnu parametrů uvedených v bodě 2.1 Externí firewall, která by vyžadovala nutnou změnu zařízení (modelu) externího firewallu.

Zadavatel požaduje službu technické a konfigurační podpory na měsíční bázi v rozsahu 8 hodin měsíčně (pomoc s konfigurací, řešení konfiguračních problémů apod.).

* 1. Školení

Součástí dodávky bude školení na dodaná zařízení v rozsahu 3 až 5 dnů s náplní odpovídající úvodnímu školení (instalace, konfigurace, řešení chybových stavů). Školení bude probíhat ve školicím středisku výrobce nebo jeho zastoupení nebo distributora v lokalitě Praha.

# **Další požadavky zadavatele**

* Zadavatel požaduje dodání originálních a nových zařízení, licencovaných ve jménu zadavatele a podle pravidel výrobce tak, aby bylo možné eskalovat případné závady přímo na lokální technickou podporu výrobce v českém nebo slovenském jazyce.
* Zadavatel požaduje oficiální potvrzení všech výrobců nabízených technologií o určení nabízených produktů HW a SW pro lokální trh.
* Zadavatel požaduje oficiální potvrzení všech výrobců nabízených technologií, že na produkty bude zajištěna podpora výrobce v místě instalace po celou dobu záruční lhůty.
* Uchazeč předloží doklad o obchodním partnerství s výrobcem zboží zaručující dostatečnou technickou podporu výrobcem.
* Zboží bude podporováno servisním střediskem výrobce na území České republiky.
* Uchazeč musí přiložit do nabídky příslušnou technickoprovozní dokumentaci výrobce zboží. Za splnění tohoto požadavku se nepovažuje odkaz na webové stránky výrobce zboží, ale dokumentace v listinné podobě nebo na datovém nosiči v anglickém nebo českém jazyce.
* Uchazeč z důvodu dodávky formou řízeného projektu velkého rozsahu a složitosti předloží jeden z následujících certifikátů a to certifikace IPMA, PRINCE2, nebo že má zaveden systém řízení podniků z hlediska řízení služeb jakosti projektů dle ISO 10006, vydaný podle českých technických norem akreditovanou osobou. Z dokladu musí být patrná doba jeho platnosti a jméno společnosti, která certifikát vydala.
* Uchazeč z důvodu dodávky, jejíž součástí je i poskytování záručního servisu na dodávaná hardwarová zařízení a softwarové produkty, předloží certifikát, že má zaveden systém řízení podniků, z hlediska řízení pro poskytování služeb IT a obsahově se řídící ustanoveními IT Infrastructure Library (ITIL) a to na úrovni minimálně jedné certifikované osoby s certifikací ITIL Foundation, vydanou podle českých technických norem akreditovanou osobou. Z dokladu musí být patrná doba jeho platnosti a jméno společnosti, která certifikát vydala.

# **Cena**

Nabídková cena bude tvořena z těchto složek:

1. Cena za externí firewall měsíčně/za 48 měsíců
2. Cena za interní firewall
3. Cena za systém zpracování logů a reporting
4. Cena za implementaci (sestavení a realizaci Implementačního plánu)
5. Cena za podporu (8 hodin) měsíčně/za 48 měsíců
6. Cena za školení

|  |  |  |
| --- | --- | --- |
| Popis | Kč/měsíc | Cena Kč (48 měsíců) |
| Cena za externí firewall | 0,00 | 0,00 |
| Cena za interní firewall | --- | 0,00 |
| Cena za systém zpracování logů a reporting | --- | 0,00 |
| Cena za implementaci (sestavení a realizaci Implementačního plánu) | --- | 0,00 |
| Cena za podporu (8 hodin) měsíčně | 0,00 | 0,00 |
| Cena za školení | --- | 0,00 |
| Celková cena |  | 0,00 |

*Ceny jsou uvedeny bez DPH.*