**Příloha č. 6 zadávací dokumentace k veřejné zakázce**

**ROZŠÍŘENÍ OCHRANY INTERNÍCH ZÓN POMOCÍ NOVÝCH FIREWALL**

**TECHNICKÁ SPECIFIKACE**

1. POPIS POŽADAVKŮ
	1. Stávající stav

V současné době řeší veškerou komunikaci mezi interními sítěmi (VLANy) dva hraniční firewally, pracující v režimu active/passive, které jsou umístěny po jednom v každém datovém centru a připojeny na páteřní přepínače.



*Schéma č. 1: Popis aktuálního stavu*

* 1. Požadovaný stav

Počítačová síť bude doplněna o dva segmentační firewally pracující v režimu active/active, které budou umístěny opět po jednom v každém datovém centru a připojeny na páteřní přepínače. Budou zajišťovat veškerou komunikaci mezi interními sítěmi a převezmou tak tuto roli z hraničních firewallů



*Schéma č. 2: Popis cílového stavu*

1. POŽADOVANÉ VLASTNOSTI A FUNKCE SEGMENTAČNÍCH FIREWALLŮ

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie vlastností** | **Požadovaný parametr nebo funkce** | **Splnění požadovaných parametrů (ANO/NE)** | **Komentář** |
| **Segmentační firewall** **(2 ks)** | Provedení pro montáž do standardního 19" rozvaděče, včetně montážní sady. |   |   |
| Maximální výška firewallu 2U. |   |   |
| Všechny porty (včetně portů pro správu a pro HA) musí být umístěny na přední straně firewallu. |   |   |
| Podpora vysoké dostupnosti v režimu active-active i active-passive. Pokud tato funkce vyžaduje licenci, pak tato musí být součástí dodávky. |   |   |
| Správa všech zařízení pracujících v režimu vysoké dostupnosti musí probíhat jednotně přes společné grafické konfigurační rozhraní. |   |   |
| Grafické konfigurační rozhraní pro správu celého clusteru, dostupné pomocí webového prohlížeče (HTTPS) bez omezení na počet administrátorů a bez nutnosti instalovat dodatečnou management platformu nebo aplikaci. |   |   |
| Minimálně 8x 10 GbE SFP+ |   |   |
| Minimálně 12x 1 GbE BASE-T (RJ-45) |   |   |
| HA port(y), pokud jsou vyhrazeny pro tento účel, musí podporovat SFP nebo SFP+ moduly pro zajištění propoje pomocí optických vláken (k dispozici jsou MM i SM vlákna), součástí dodávky musí být i potřebné optické moduly. |   |   |
| Pokud zařízení nemá vyhrazené HA porty, navyšuje se požadavek na minimální počet portů příslušného typu o počet portů nutných k zajištění funkce HA. |   |   |
| Konzolový port pro management. |   |   |
| Dedikovaný port RJ-45 pro management. |   |   |
| Redundantní, za provozu vyměnitelné napájecí zdroje 230V AC. |   |   |
| Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené specializovanými obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání s databází signatur apod.). |   |   |
| Zařízení může pracovat buď v L2 režimu (transparentní režim inspekce) nebo L3 režimu (NAT/router režim s inspekcí). |   |   |
| Podpora překladu adres (NAT). |   |   |
| Modul funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén, databáze automaticky aktualizované výrobcem). |   |   |
| Funkce rozpoznávání populárních síťových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet definice pro vlastní aplikace. |   |   |
| Funkce ochrany před síťovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů. |   |   |
| Funkce dynamického routingu (min. BGP, OSPF, RIP, PIM), pokud jsou tyto funkce licencované, pak licence musí být součástí dodávky. |   |   |
| Funkce QoS, traffic shaping, rate-limiting pro jednotlivé aplikace. |   |   |
| Podpora automatické karantény klientů klasifikovaných firewallem jako problematické. |   |   |
| Všechny provozní funkce musí být dostupné pro protokoly IPv4 i IPv6. |   |   |
| Podpora virtuálních LAN dle IEEE 802.1Q |   |   |
| Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad |   |   |
| Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) |   |   |
| Podpora odesílání log zpráv na externí syslog server. |   |   |
| Podpora analýzy síťového provozu (Netflow nebo sFlow nebo IPFIX) |   |   |
| Minimální požadovaná propustnost firewallu pro IPv4 i IPv6 provoz je na 64B paketech 68 Gbps. |   |   |
| Při měření na provozu tvořeným mixem různě velkých paketů, nebo při měření na malých (64B) paketech, nesmí výkonnost poklesnout pod 50 %. |   |   |
| Latence FW pod 5 µs. |   |   |
| Počet současně navázaných spojení firewallu minimálně 7M, počet nových spojení za sekundu minimálně 450k. |   |   |
| Propustnost funkcí next generation firewallu (stavový firewall, IPS, analýza aplikací) minimálně 8.5 Gbps (měřeno na provozu simulujícím reálnou komunikaci/real world traffic). |   |   |
| Propustnost funkcí ochrany před škodlivým kódem (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) minimálně 8 Gbps (měřeno na provozu simulujícím reálnou komunikaci/real world traffic). |   |   |
| Schopnost staticky definovat filtrační síťová pravidla do FW (ACL). |   |  |
| **Připojení k páteřním prvkům** | Propoje o minimální kapacitě 20 Gbps z každého segmentačního firewallu do páteřních switchů v každém datovém centru, součástí dodávky musí být odpovídající optické transceivery kompatibilní s nabízeným zařízením a optické patch kabely pro SM optiku (OS2, délka 5m), optická vlákna jsou zakončena na SC konektorech |   |   |
| **Připojení ke switchům pro servery** | 6x 10G SFP+ modul pro multimode optiku, kompatibilní s nabízeným firewallem (připojení switchů pro servery) |   |   |
| 2x 10G SFP+ modul pro singlemode optiku, kompatibilní s nabízeným firewallem (připojení switchů pro servery) |   |   |
| 4x optický duplexní patch kabel LC-LC OM4 délka 5 m |   |   |
| 4x optický duplexní patch kabel LC-SC OM4 délka 5 m |   |   |
| 2x optický duplexní patch kabel SC-SC OM4 délka 2 m |   |   |
| 4x optický duplexní patch kabel LC-SC OS2 délka 5 m |   |   |
| 2x optický duplexní patch kabel SC-SC OS2 délka 2 m |   |   |
| **Školení** | Školení správců v minimálně délce 16 hodin. |   |   |
| **Instalace a konfigurace** | Instalační a konfigurační práce včetně migrace a optimalizace stávajících pravidel pro interní provoz z firewallu Sophos XGS 2300 |   |   |
| **Licence** | Všechny potřebné licence pro provoz na dobu minimálně 5 let. |   |   |
| **Záruka** | Záruka na hardware minimálně 5 let, řešení opravy formou výměny zařízení s odesláním následující pracovní den po identifikaci a uznání závady výrobcem |   |   |
| **Podpora** | Podpora na hardware minimálně 5 let, v režimu min. 8x5, standardně dostupná prostřednictvím telefonní linky nebo webového portálu pro správu požadavků, včetně přístupu k aktualizacím SW a novým funkcionalitám |   |   |

1. DALŠÍ SLUŽBY
	1. Projektové řízení

Zadavatel požaduje zajištění projektového vedení realizace předmětu plnění. Dodavatel zajistí projektové vedení po celou dobu realizace zakázky. Dodavatel zajistí:

* 1. Projektové vedení plnění předmětu plnění po celou dobu realizace dodávky prostřednictvím projektového manažera, který bude v průběhu plnění aktivně a konstruktivně komunikovat se jmenovaným zástupcem zadavatele;
	2. proaktivní vyžádání si součinnosti a koordinace prací, služeb a/nebo dodávek třetích stran (zejm. stávajících dodavatelů zadavatele) zapojených do plnění za účelem dosažení úspěšné realizace předmětu plnění veřejné zakázky jako celku a jeho úspěšné realizace v daném časovém rámci vč. jednotlivého oprávněného konkrétního úkolu s určeným termínem z kontrolního dne v rámci koordinace prací, služeb a/nebo dodávek;
	3. organizaci kontrolních dnů – kontrolní dny se budou konat za účasti zástupců dodavatele a zadavatele min. 1 x 14 dní; dodavatel zajistí řízení všech kontrolních dnů a dílčích jednání se členy realizačního týmu na straně zadavatele;
	4. zpracování harmonogramu prací v podobě navazujících činností, např. formou Ganttova diagramu nebo MS Project, či obdobného nástroje postihujícího návaznosti ke všem částem plnění;
	5. řízení vzniku veškeré provozně-technické dokumentace, školících materiálů pro školení administrátorů, organizace školení samotného a další projektové dokumentace;
	6. veškeré řídící činnosti projektu s vlastníky projektu na straně zadavatele nebo jím určených třetích stran na straně dodavatele.
	7. Školení

Zadavatel v rámci dodávky požaduje proškolení 2 správců v rozsahu nezbytném pro zajištění standardního provozu a správy dodaných segmentačních firewallů, min. však v délce 16 hodin.

* 1. Rozsah implementace

Náklady na provedení instalačních a implementačních prací musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Zadavatel požaduje provedení prací minimálně v níže uvedeném rozsahu.

* Doprava veškerého hardware do místa instalace, sídla zadavatele.
* Asistence při přípravě a konfiguraci firewallů
* Migrace a optimalizace stávajících pravidel pro interní provoz z firewallu Sophos XGS 2300
* Přítomnost kvalifikovaného pracovníka dodavatele v místě instalace při nasazení segmentačních firewallů do ostrého provozu.
	1. Testovací provoz (akceptační testy)

Zhotovitel v rámci realizace předmětu smlouvy vypracuje návrh testovacích postupů pro ověření funkčnosti díla a vypracuje jednotlivé akceptační protokoly. Návrh testovacích postupů bude předložen objednateli a po jeho schválení bude objednatelem akceptován.

Testovací postupy se musí týkat minimálně těchto oblastí:

* vysoká dostupnost (HA),
* síťová pravidla, NAT,
* bezpečnostní funkce (IPS, analýza aplikací, ochrana před škodlivým kódem),
* dohled a napojení na SIEM (SNMP, syslog),
* výkonnostní parametry.

**Funkční testy**

Funkční testy ověří, že implementované řešení poskytuje bezchybně všechny požadované funkcionality uvedené v Technické specifikaci.

Testovací provoz bude probíhat v sídle objednatele minimálně v délce 30 dní.

* 1. Požadavky na dokumentaci

**Dodavatel zpracuje komplexní a detailní řešení nasazení díla**, a to ve vazbě na požadavky uvedené v této technické dokumentaci. Cílem je zpracování dokumentu v takové míře detailu jednotlivých postupů a prací zasazení do prostředí a jeho nastavení, která umožní dosažení zavedení řešení do rutinního provozu řízenou formou. Dokument proto bude jednoznačně a jasně konkretizovat jednotlivé kroky prací a to min. v rozsahu, které kroky a jakým způsobem budou řešeny, kým budou řešeny, za jaké součinnosti objednatele a v jakém čase. Taková konkretizace bude dále dodržovat časovou, věcnou a logickou souslednost a bude z ní tedy možné v každém okamžiku realizace jednotlivých částí díla určit, co je právě realizováno a v jakém stavu a co bude následovat.

Objednatel bude moci na základě takových podkladů alokovat své potřebné kapacity na součinnost a průběžnou kontrolu plnění díla. Bez odsouhlasené prováděcí dokumentace ze strany objednatele, tedy shody objednatele a zhotovitele na způsobu a formě nasazení jednotlivých částí díla nebude moci být započata implementace.

**Dodavatel zpracuje provozně-technickou dokumentaci v rozsahu** dokumentace skutečného provedení a provozní dokumentace.

Dokumentace skutečného provedení musí obsahovat minimálně tyto části:

* detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému;
* seznam dodaného hardware, jeho produktových čísel a dalších podrobností (např. sériových čísel, MAC adres, IP adres a umístění apod.);
* seznam všech zařízení, rozhraní a jejich MAC adres a k nim odpovídajících IP adres použitých v nové infrastruktuře;
* detailní popis zajištění bezpečnosti informací;
* detailní popis designu řešení a jeho konfigurace;
* vazby na stávající infastrukturu a/nebo systémy a jejich konfigurace.

**Provozní dokumentace bude obsahovat instrukce a postupy pro administrátory a bezpečnostní správce zařízení.**

**Dodavatel dále zpracuje projektovou dokumentaci v rozsahu odpovídajícím předmětu plnění, zejména pak zápisy z kontrolních dnů a projektových porad a další odpovídající podklady nebo dokumenty související s plněním a dodáním předmětu plnění.**

* 1. Záruka, podpora a servis

Záruka na hardware minimálně 5 let, řešení opravy formou výměny zařízení s odesláním následující pracovní den po identifikaci a uznání závady výrobcem

Standardní záruční podpora na hardware minimálně 5 let, v režimu min. 8x5, standardně dostupná prostřednictvím telefonní linky nebo webového portálu pro správu požadavků, včetně přístupu k aktualizacím SW a novým funkcionalitám.

1. POIMPLEMENTAČNÍ PODPORA

Zadavatel požaduje poskytnutí poimplementační technické podpory dodaného řešení proškoleným zaměstnancům zadavatele (administrátorům). Podpora bude využita zejména pro potřeby následného provozu a správy dodaných technologií a dodaného řešení.

* Požadovaný rozsah technické podpory – 8 hodin po dobu 3 měsíců od finální akceptace dodaného řešení.
* Technická podpora může být poskytována i vzdáleně (např. MS Teams) nebo telefonicky.
* Technická podpora bude dostupná v pracovní době od 7:00 do 16:00.
* Podpora bude poskytována technickým specialistou, který byl součástí realizačního týmu, případně technickým specialistou odpovídající kvalifikace.

Požadavek na podporu bude možné zadat prostřednictvím helpdeskového systému dodavatele nebo e-mailem, příp. telefonicky.

1. HARMONOGRAM

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti Smlouvy o dílo. Čísla značí počet kalendářních dnů.

| **Aktivita** | **Začátek** | **Termín splnění** |
| --- | --- | --- |
| Nabytí účinnosti smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+7 |
| Předimplementační analýza – zpracování | D+7 | D+17 |
| Předimplementační analýza – připomínkové řízení, schválení | D+17 | D+24 |
| Prováděcí dokumentace – zpracování | D+24 | D+34 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+34 | D+48 |
| Realizace předmětu plnění | D+48 | D+100 |
| Školení administrátorů | D+48 | D+100 |
| Testovací provoz | D+100 | D+120 |
| Akceptační testy | D+100 | D+120 |
| Zahájení ostrého provozu | D+121 |  - |

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

**Detailní harmonogram plnění uvede dodavatel ve své nabídce.**

**Dodavatel uvede ve své nabídce (jako součást harmonogramu) požadovanou součinnost zadavatele pro splnění harmonogramu plnění.**