Klasifikace: Veřejný dokument

SPRÁVA ŽELEZNIC

Technická specifikace

Příloha č. 1 zadávací dokumentace „Ochrana perimetru a DMZ – Next Generation Firewall"

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

Obsah

1 Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

Zkratka	Popis
DMZ	Demilitarizovaná zóna
IT	informační technologie
Gbps	gigabit per second
IPS	Intrusion Prevention System
URL	Uniform Resource Locator
SSL	Secure Socker Layer
TLS	Transport Layer Security
IP	Internet Protocol
TCP	Transmission Control Protocol
IPsec	IP security
DoS	Denial of Service
DDoS	Distributed Denial of Service
LDAP	Lightweight Directory Access Protocol
NTLM	New Technology LAN Manager
RADIUS	Remote Authentication Dial In User Service
TACASC	Terminal Access Controller Access-Control System
SSO	Single Sign On
NAT	Network Address Translation
GB	Gigabyte
DNS	Domain Name System

HW	Hardware
NTP	Network Time Protocol
VLAN	Virtual Local Area Network
DHCP	Dynamic Host Configuration Protocol
FQDN	Fully Qualyfied Domain Name
SIEM	Security Information and Event Management
NBD	Next Bussines Day
OS	Operation System
MD	Man-Day

2 Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace týkající se veřejné zakázky s názvem „Ochrana perimetru a DMZ – Next Generation Firewall" (dále jen „veřejná zakázka"), pro organizaci Správa železnic, státní organizace (dále jen „SŽ" nebo "Zadavatel"). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

Technická specifikace je závazná a její nedodržení je důvodem k vyloučení dodavatele ze zadávacího řízení.

2.1 Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je dodávka technologie Next Generation Firewall pro ochranu externího perimetru IT sítě Zadavatele, implementace a konfigurace dodané technologie a odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele. Nedílnou součástí plnění je také technická podpora dodaných technologií, pravidelné bezpečnostní aktualizace bezpečnostních funkcionalit a post-implementační podpora Zadavatele.

Tato veřejná zakázka bude obsahovat následující poptávané oblasti:

- Dodávka technologií a licencí
- Implementační práce
- Odborné školení správy a údržby dodaných technologií
- Post-implementační a technická podpora
- Konzultační služby na vyžádání.

3 Požadavky na plnění

Plnění Veřejné zakázky se musí skládat alespoň z níže uvedených částí:

1. Dodávka čtyř zařízení Next Generation Firewall
2. Dodávka zařízení pro centrální správu dodávaných Next Generation Firewallů
3. Implementace Next Generation Firewallu na externím perimetru sítě
4. Implementace zařízení na centrální správu
5. Odborné školení
6. Post-implementační a technická podpora
7. Konzultační služby na vyžádání.

Vyloučení technologií představujících kybernetickou hrozbu

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: „Použití technických nebo

programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:

- *Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*
- *ZTE Corporation, Šen-čen, Čínská lidová republika".*

Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika"), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou Zadavatel provedl analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů. V návaznosti na to Zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

Zadavatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

3.1 Dodávka čtyř zařízení Next Generation Firewall

V oblasti dodávky čtyř zařízení Next Generation Firewall definuje Zadavatel následující požadavky pro každé z nich:

Oblast	Požadavek
Typ zařízení	Fyzické ve standardním provedení do rozvaděče o šířce 19 palců.
Rozhraní s přenosovou rychlostí 40 Gbps	Minimálně 2.
Rozhraní s přenosovou rychlostí 10 Gbps	Minimálně 2.
Propustnost provozu při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	Minimálně 9 Gbps provozu označovaného jako „Enterprise Mix traffic".
Propustnost SSL/TLS inspekce	Minimálně 4 Gbps.
Podpora protokolu TLS inspekce	Minimálně TLS 1.2 a TLS 1.3.

Explicitní proxy	Možnost konfigurace firewallu jako explicitní proxy. Tedy konfigurace internetových prohlížečů a dalších aplikací koncových zařízení na dedikovanou proxy IP adresu a TCP port.
Interní virtualizace	Zařízení budou rozdělena na dva samostatné klastry, každý klastr po dvou nodech. Každý klastr musí být možné rozdělit minimálně na 5 samostatných administrativně nezávislých virtuálních zařízení, a to bez nutnosti pořízení dodatečné licence.
Sandbox analýza (Cloud)	Možnost odesílání podezřelých souborů identifikovaných pokročilou detekcí na ochranu proti malwaru do sandbox prostředí výrobce umístěného v cloudovém prostředí. Konfigurace firewallu musí umožňovat granulární řízení, ze kterých datových toků je odesílání souborů k analýze povoleno.
Propustnost IPsec	Minimálně 10 Gbps.
Podpora pravidel na základě identit uživatelů	Firewallová pravidla umožňují řízení provozu na základě uživatelské identity a uživatelských skupin, ve kterých je uživatelská identita členem.
Způsoby ověřování uživatelů či napojení na autentizační systémy	Podpora proaktivního ověřování pomocí protokolu LDAP, NTLMv2, RADIUS a TACASC+. Dále je požadována SSO funkcionalita na základě proaktivního vyčítání událostí o přihlášení ze systému Active Directory.
Módy vysoké dostupnosti klastru	Podpora režimů Active-Active a Active-Passive.
Podpora NAT64	Zařízení musí disponovat možností překladu IPv6 adres na IPv4 adresy.
IPS	Systém pro detekci a prevenci průniku s automatickou bezpečnostní aktualizací z cloudové služby výrobce s minimálním počtem 10000 jedinečných signatur.

Aplikační kontrola	Detekce a řízení síťových aplikací. Minimálně 4000 rozpoznávaných aplikací.
URL filtrace	Automatické řízení přístupů k webovým službám na základě reputace a kategorií.
Antivirus	Ochrana před škodlivým softwarem procházejícím firewall v reálném čase.
Směrování provozu	Podpora statického, policy based a dynamického směrování provozu.
Velikost lokálního úložiště	Minimálně 100 GB.
Další požadované funkcionality	Antibot, Ochrana DNS.

Zadavatel požaduje, aby byla dodávaná technologie umístěna v pozici Leaders v průzkumech nezávislých a celosvětově odbornou komunitou uznávaných společností Gartner nebo Forrester. Konkrétně se jedná o umístění v kvadrantu "Leaders" v hodnocení Gartner Magic Quadrant for Network firewalls z roku 2022 nebo Forrester Wave Enterprise Firewalls z roku 2022.

Zařízení Next Generation Firewall musí být dodána včetně veškerých potřebných licencí.

3.2 Dodávka zařízení pro centrální správu dodávaných Next Generation Firewallů

V oblasti dodávky zařízení pro centrální správu dodávaných Next Generation Firewallů definuje Zadavatel následující požadavky:

Oblast	Požadavek
Typ zařízení	Zařízení může být realizováno jako fyzické nebo virtualizované pro virtualizační platformu VMware.
Počet spravovaných zařízení	Zařízení na centrální správu musí umožnit správu minimálně 10 logických či fyzických zařízení bez dalšího licenčního omezení.
Práce s událostmi	Zařízení na centrální správu umožňuje příjem a úchovu událostí v minimálním množství 10 GB událostí za den s možností licenčního rozšíření minimálně na 50 GB událostí za den.

Pokročilá analýza událostí	Zařízení na centrální správu umožňuje pokročilou analýzu událostí za účelem včasné identifikace reálné či potencionální hrozby.

Zařízení pro centrální správu dodávaných Next Generation Firewallů musí být dodána včetně veškerých potřebných licencí.

3.3 Implementace Next Generation Firewallu na externím perimetru sítě

V oblasti implementace Next Generation Firewallu na externím perimetru sítě jsou definovány následující činnosti, resp. požadavky:

Oblast	Činnost
Dodávka zařízení	Zadavatel požaduje dodávku všech zařízení do lokality Praha s následných převozem 2 ks zařízení do lokality Plzeň po dokončení základní konfigurace zařízení.
Základní konfigurace	- Ověření zařízení na absenci HW vad - Registrace zařízení - Instalace výrobcem doporučené verze operačního systému ○ Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).
Virtuální kontexty	Rozdělení firewallu na 3 logické firewally.
Konfigurace clusteru	Nasazení dvou klastrů v režimu Active-Pasive.
Síťová konfigurace	- Linková agregace - IP adresace a VLAN tagy - Směrování - DHCP relay.
Přenos objektů a bezpečnostní politiky	- Migrace 4200 pravidel ze zařízení Cisco ASA - Migrace 1000 objektů (IP adresy, FQDN, skupiny apod.) - Hygiena pravidel (například překrývající se pravidla).
Definice vzorových bezpečnostních politik dle	- IPS - Antimalware - Anti-DDoS

požadavků Zadavatele	- Application Control - Web Filtering.
SSO Autentizace	Napojení na Active Directory řízení přístupů na základě identit.

3.4 Implementace zařízení na centrální správu

V oblasti implementace zařízení na centrální správu jsou definovány následující činnosti, resp. požadavky:

Oblast	Činnost
Dodávka zařízení	Dodávka zařízení do lokality Praha. V případě virtualizovaného zařízení poskytnutí instalačních dat skrze internetovou konektivitu.
Základní konfigurace	- Ověření zařízení na absenci HW vad (pouze u fyzického zařízení) - Registrace zařízení - Instalace výrobcem doporučené verze operačního systému. o Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).
Připojení spravovaných zařízení	Integrace dodaných Next Generation Firewallů do centrální správy.

3.5 Odborné školení

V oblasti odborného školení jsou definovány, resp. požadovány následující dva typy školení:

Typ školení	Popis
Hands-On školení	Dodavatel provádí implementaci definovanou v kapitolách 3.3 a 3.4 této Technické specifikace ve formě slovního průvodce, kdy veškeré činnosti provádí zástupce Zadavatele. Jednotlivé kroky implementace jsou zástupci Zadavatele podrobně popsány tak, aby

	došlo k ideální konfiguraci pro dané prostředí Zadavatele.
Výrobcem certifikované školení	Dodavatel zajistí pro 5 zástupců Zadavatele odpovídající výrobcem certifikované školení dodávané technologie, které odpovídá požadavkům na každodenní správu a údržbu zařízení, správu z pohledu kybernetické bezpečnosti a kybernetického monitoringu (například představení kybernetických funkcionalit, jejich napojení na dohledové nástroje typu SIEM a využití NGFW pro forenzní šetření). Školení v rozsahu minimálně 3 dny. Školení nemusí být zakončeno certifikační zkouškou.

3.6 Post-implementační a technická podpora

V oblasti post-implemetační a technické podpory jsou definovány následující požadavky:

Oblast	Požadavky
Oficiální podpora výrobce	Dodavatel zajistí oficiální podporu výrobce po dobu 5 let od dodávky technologií a licencí, která zahrnuje minimálně: - Režim podpory 8x5x4 (8 hodin denně v rámci pracovních dní, reakční doba 4 hodiny) - Doručení vadného dílu v režimu NBD - Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu - Přístup k novým verzím firmware či OS - Aktualizace bezpečnostních definic pro funkcionality definované v kapitole 3.1.
Podpora dodavatele	Dodavatel zajistí podporu po dobu 5 let dle paramentů a za podmínek uvedených v příloze č. 4 zadávací dokumentace - Závazném vzoru smlouvy a jejích přílohách (zejména Zvláštní obchodní podmínky pro zakázky v oblasti ICT).

3.7 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

Oblast	Požadavky
Konfigurační konzultace	Dodavatel zajistí certifikovaného odborníka v oblasti dodané technologie, který Zadavateli umožní konzultovat konfigurační parametry dodaného řešení. Požadovaný počet MD k čerpání: 5
Analytická konzultace	Dodavatel zajistí certifikovaného odborníka v oblasti vyšetřování kybernetických událostí v rámci dodané technologie pro konzultace bezpečnostních nálezů identifikovaných dodaným řešením. Požadovaný počet MD k čerpání: 5

Maximální limit MD k čerpání v součtu pro konfigurační konzultace a analytické konzultace je 10 MD.

4 Fáze dodávky a akceptační milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být Zadavatelem separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané Fáze, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je dodavatel povinen napravit nedostatky plnění.

Fáze	**Popis**	**Kapitola obsahující požadavky**
F1	Dodávka: - čtyř zařízení Next Generation Firewall, včetně potřebných licencí a podpory výrobce - zařízení pro centrální správu dodávaných Next Generation Firewallů, včetně potřebných licencí a podpory výrobce	3.1, 3.2 a 3.6
F2	Implementační práce: - Next Generation Firewallu na externím perimetru sítě - zařízení na centrální správu,	3.3, 3.4
F3.a	Školení: - Hands-On školení	3.5 (Pro Hands-On školení jsou validní požadavky na

Fáze	Popis	Kapitola obsahující požadavky
		implemetace, kapitoly 3.3 a 3.4.)
F3.b	Školení: - Výrobcem certifikované školení	3.5
F4.a	Post-implemetační a technická podpora - Oficiální podpora výrobce	3.6
F4.b	Post-implemetační a technická podpora - Podpora dodavatele	3.6
F5	Konzultační služby na vyžádání	3.7