Příloha ke Kupní smlouvě - Technická specifikace k VZ "Nový NGFW firewall"

Takto podbarvená pole dodavatel povinně vyplní

Předmětem zakázky je pořízení nového NGFW (next-generation firewall) firewallu ve failover režimu.

V rámci plnění je požadováno poskytnutí a implementace komplexních bezpečnostních opatření na perimetru počítačové sítě Zadavatele, jejíž součástí budou následující služby a dodávky:

- dodávky dvou firewallů NGFW včetně poskytnutí dvou provozních licencí na dobu 36 měsíců, bude-li to s ohledem na nabízené řešení vyžadováno,
- implementace systému v režimu vysoké dostupnosti HA, včetně konzultace a optimalizace nastavení,
- implementace centrální správy managementu NGFW,
- implementace IPS,
- zaškolení ovládání SW prostředí,
- služby výše uvedené v rozsahu min. 4MD (32 hodin).

V databázi výrobce musí být Kupující veden jako první uživatel zboží a licencí/subscripcí/operačních systémů. **Kupující požaduje originální a nová zařízení určená pro evropský trh.** Při předání zboží proběhne kontrola dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Kupující, bude se jednat o porušení podmínky originálního a nového zařízení.

Součástí nabídky musí být odkaz na veřejně dostupné webové stránky výrobce, nebo jiná forma potvrzení výrobcem, z jejichž obsahu bude nadevší pochybnost zřejmé, že výrobce nabízených aktivních síťových prvků má implementován tzv. “SDL - secure development lifecycle“ při vývoji svých produktů a tzv. “SIRT - Security Incident Response Team” pro reportování bezpečnostních incidentů spojených s nabízenými produkty (viz prostor pro prokázání níže).

Servisní podpora

Požadujeme záruku po dobu 36 měsíců od předání na veškerý dodaný hardware a software včetně platnosti licencí. Tato záruka musí zahrnovat výměnu vadného dílu do příštího pracovního dne od ohlášení závady (8x5xNBD), nárok na nové verze programového vybavení zakoupené funkční sady a nárok na podporu Technical Assistance Center (TAC) výrobce.

Zadavatel definuje následující vlastnosti, které musí nabízené řešení splňovat:

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Dodavatel doplní konkrétní hodnoty dle nabízeného zařízení
Výkon a funkcionalita firewallu:		
Formát zařízení	Appliance, 1RU	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1	1
Minimální počet 10Gb SFP+ rozhraní portů pro data, standardně osazených	4	4
Možnost rozšíření o moduly rozhraní	min. 1	1
Možnost rozšíření o další 10Gb SFP+ rozhraní	min. 8	8
Redundantní zdroje	Ano	ANO
Podporovaný počet současně otevřených spojení aplikační FW/stavový FW	min. 2M/2M	2M/2M
Rychlost vytváření nových spojení přes stavový FW	min. 27K	30K
Propustnost stavového firewallu (multiprotokolový režim)	min. 5 Gbps	5,4 Gbps
Propustnost aplikačního FW (NGFW) – (top parametry)	min. 5 Gbps	5,4 Gbps
Propustnost aplikačního FW + IPS (NGFW, IPS) - (top parametry)	min. 5 Gbps	5,4 Gbps
Dešifrování TLS (HW podpora)	min. 735 Mbps	760 Mbps
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano	ANO
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	ANO
Podporovaný počet VLAN	Min. 1024	1024

Podpora stateful failover	active/standby	ANO
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano	ANO
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano	ANO
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP	Ano	ANO
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	Ano	ANO
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	ANO
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	ANO
Podpora Policy based Routing	Ano	ANO
Podpora kontroly paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	ANO
Podpora filtrace IPv4, IPv6	Ano	ANO
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	ANO
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	ANO
Podpora inspekce IPv6 provozu	Ano	ANO
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	ANO
Podpora NAT64 a DNS64	Ano	ANO
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na	Ano	ANO

škodlivý kód připadně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.		
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano	ANO
Možnost rozšíření o funkce NGFW	Ano	ANO
Možnost rozšíření o funkce NextGen IPS	Ano	ANO
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	ANO
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	ANO
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	ANO
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	ANO
Funkce IPS a anti-malware:		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	ANO
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	ANO
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	ANO
Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podpora různých IPS politik pro různé typy provozu	Ano	ANO
Inspekce pro IPv4 a IPv6	Ano	ANO
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	ANO
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity,	Ano	ANO

ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií		
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	ANO
Podpora aplikace pro psaní zákaznických filtrů	Ano	ANO
Podpora importu komunitních filtrů/signatur Snort	Ano	ANO
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	ANO
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	ANO
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano	ANO
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano	ANO
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	ANO
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	ANO
Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	ANO
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	ANO
Možnost definice uživatelské vrstvy politik	Ano	ANO

Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	ANO
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	ANO
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano, dokoupením licence	Ano, dokoupením licence
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano, dokoupením licence	Ano, dokoupením licence
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano, dokoupením licence	Ano, dokoupením licence
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano, dokoupením licence	Ano, dokoupením licence
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano, dokoupením licence	Ano, dokoupením licence
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	Ano, dokoupením licence	Ano, dokoupením licence
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano, dokoupením licence	Ano, dokoupením licence
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	ANO

Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	ANO
Možnost automatické i manuální klasifikace stanice jako “kritické” se zohledněním v pravidlech, reportech apod.	Ano	ANO
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	ANO
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	ANO
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	ANO
Funkce Next-Generation Firewall:		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	ANO
Podpora pasivního monitorování (TAP režim)	Ano	ANO
Podpora 802.1Q tagovaných rámců	Ano	ANO
Podporovaných aplikací	Min. 3000	3000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	ANO
Filtrace podle typů aplikací	Ano	ANO
Možnost integrovat vlastní reputační databáze	Ano	ANO
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano	ANO
Filtry mohou zohlednit roli a identitu uživatele	Ano	ANO
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	ANO
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	ANO

Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:	Typ zařízení	ANO
	Operační systém	ANO
	Dodavatel OS	ANO
	Použité síť. protokoly	ANO
	Použité síť. služby	ANO
	Otevřené porty síť. služeb	ANO
	Potenciální zranitelnosti	ANO
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow	ANO
	Akce (allow, deny,..)	ANO
	Důvod případného blokování	ANO
	Zdroj. a cíl. adresa	ANO
	Vstupní a výstupní zóna	ANO
	Vstupní a výstupní rozhraní	ANO
	Zdroj. a cíl. port	ANO
	Aplikační protokol	ANO
	IPS událost, pokud vznikne	ANO
	Riziková úroveň IPS události	ANO
	Použitá síťová aplikace	ANO
	Rizikovost aplikace	ANO
	„Business impact“ aplikace	ANO
	Množství přenesených dat	ANO
Odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu je zřejmé, že výrobce má implementován tzv. „SDL – secure development lifecycle“ při vývoji svých produktů a tzv. „SIRT – Security Incident Response Team“ pro reportování bezpečnostních incidentů. Pokud výrobce tyto informace na webových stránkách nemá, pak doložte jinou formu potvrzení výrobcem, např. jako přílohu nabídky.		
Vypište: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf		

Označení nabízeného zboží (Přesný typ / produktové číslo, nebo odkaz na webové stránky produktu vedoucí k přesné identifikaci nabízeného řešení)	
Dodávka NGFW firewall	FPR2130-NGFW-K9 - Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay
Provozní licence (na dobu 36 měsíců)	L-FPR2130T-T-3Y - Cisco FPR2130 Threat Defense Threat Protection 3Y Subs
Redundantní napájecí zdroj	FPR2K-PWR-AC-400 - Firepower 2000 Series 400W AC Power Supply
Záruční servis v délce min. 36 měsíců pro obě zařízení	Servisní služby - Dodávka náhradního dílu do následujícího pracovního dne (8x5xNBD), nárok na nové verze SW v rámci zakoupené licence, podpora Cisco TAC, 36 měsíců

Nabídková cena

Nabídková cena celkem v Kč bez DPH	
Dodávka NGFW firewall - 2x	506 284,00 Kč
Provozní licence (na dobu 36 měsíců) – 2x	176 558,00 Kč
Redundantní napájecí zdroj – 2x	40 968,00 Kč
Instalace, konzultace, zaškolení obsluhy (min. 32 hodin celkem)	48 000,00 Kč
Záruční servis v délce min. 36 měsíců pro obě zařízení (viz specifikace výše)	133 858,00 Kč
CENA CELKEM v Kč bez DPH	**905 668,00 Kč**

Dodavatel svým podpisem potvrzuje splnění všech výše uvedených podmínek, požadavků a nabídkovou cenu.

Ing. Jan Šíp, prokurista