**Příloha č. 3 zadávací dokumentace ve veřejné zakázce**

„Dodávka NG Firewall“

**Technická specifikace**

**Předmětem plnění veřejné zakázky je dodávka dodání 2 kusů NG Firewallů nasazené v režimu Active-Active.**

|  |  |
| --- | --- |
| **ZÁKLADNÍ TECHNICKÉ POŽADAVKY** | **Nabízená dodávka splňuje (ANO x NE)** |
| Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …). |  |
| Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky (uzavření smlouvy) v režimu End of Sales / End of Support. |  |
| Všechny požadované funkce musí být v době podání nabídky (uzavření smlouvy) součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. |  |
| Dodávka zařízení ve formátu HW appliance o velikosti 1 RU |  |
| Dodávka veškerého příslušenství (montážní prvky) pro montáž do RACK |  |
| Dodávka 4 originálních SFP+ modulů (10GBase-SR) |  |
| Možnost rozšíření platformy o další prvek typu NGFW, jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem. |  |
| Možnost rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality. |  |

|  |  |
| --- | --- |
| **HW PARAMETRY** | **Nabízená dodávka splňuje (ANO x NE) + uvedení hodnoty** |
| Počet síťových rozhraní copper, RJ45 10/100/1000 (min 18x) |  |
| Počet 10 GE SFP+ (min 2x) |  |
| Počet GE SFP (min 4x) |  |
| Dedikovaný port RJ45 pro management |  |
| Dedikovaný port RJ45 pro DMZ |  |
| USB 3.0 port pro zálohu konfigurace |  |
| Redundantní napájecí zdroj |  |

|  |  |
| --- | --- |
| **VÝKONNOSTNÍ PARAMETRY** | **Nabízená dodávka splňuje (ANO x NE)** |
| Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B - min. 18000 Mbps, 16000 Mbps, 9000 Mbps |  |
| Latence firewallu (64 B UDP paket) – max. 7 mikro sec |  |
| Výkon firewall – 14000000 paketů / s |  |
| Počet naráz otevřených spojení – min. 1.3 M |  |
| Počet nových spojení za sekundu - min. 52 000 |  |
| Počet firewall pravidel až 10 000 |  |
| Podpora virtualizace (min 10 virtuálních kontextů) |  |
| Podpora funkce bezdrátový kontrolér - 64 AP |  |
| Podpora funkce integrovaný switch controller – podpora až 24 switchů |  |

|  |  |
| --- | --- |
| **Funkce:****NETWORKING A HIGH AVAILIBILITY** | **Nabízená dodávka splňuje (ANO x NE)** |
| Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru |  |
| Režim fungování L2 – transparentní režim, L3 – NAT/Router |  |
| Podpora VLAN |  |
| Podopora multicast, vytváření politiky pro multicast routování |  |
| Podpora 802.3ad link aggregation |  |
| Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading |  |
| Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace |  |
| Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP |  |
| Policy-based routing |  |
| Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky |  |

|  |  |
| --- | --- |
| **Funkce:****VPN** | **Nabízená dodávka splňuje (ANO x NE)** |
| **Funkce SSL VPN** | **-** |
| Podpora klientského i bezklientského (portálového) režimu |  |
| Minimální počet současně navázaných SSL VPN tunelů: 450 |  |
| Minimální propustnost SSL VPN: 900Mbps |  |
| **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: 2300 |  |
| Minimální počet klientských IPSEC VPN tunelů: 15000 |  |
| Propustnost IPSec VPN min. 11Gbps (měřeno při AES256-SHA256) |  |
| Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování |  |
| Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování |  |
| Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace |  |
| Podpora VXLAN |  |
| Podpora L2TP, PPTP, GRE |  |
| Podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec |  |
| **Funkce:****UTM** | **Nabízená dodávka splňuje (ANO x NE)** |
| **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 akce 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. |  |
| **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. 1500Mbps (měřeno na komunikaci typu mix aplikací) |  |
| **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 lokálné HW appliance stejného výrobce |  |
| Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 650 Mbps |  |
| Funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. |  |
| Podpora služby výrobce, která umožní́ detekovat malware, který byl objevený v době od poslední́ aktualizace AV signaturové databáze pomocí globální́ a rychle se aktualizující́ databáze hashů. |  |
| Funkce odstranění́ aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní́ 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. |  |
| **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 |  |
| **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 |  |
| Detekce a blokování komunikace do botnet sítí |  |
| **Funkce ochrany 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 |  |
| E-mail filter – jednoduchá antispamová a antivirová inspekce elektronické pošty |  |
| Podpora SSL dekrypce / SSL inspekce s minimální propustností 900Mbps |  |
| DoS Policy prevence proti základním útokům typu DoS |  |
| **Základní technické požadavky****FIREWALL** | **Nabízená dodávka splňuje (ANO x NE)** |
| Možnost nastavovat firewall politiku na základě geografických údajů |  |
| Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem |  |
| Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud |  |
| Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru |  |
| Viditelnost do provozu na aplikační úrovni |  |
| 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). |  |
| Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu |  |
| Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. |  |
| Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii |  |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu |  |
| Podpora funkce reverzní proxy |  |
| Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů |  |
| **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 |  |

|  |  |
| --- | --- |
| **Základní technické požadavky****INTEGROVANÝ CONTROLLER BEZDRÁTOVÝCH (WIFI) SÍTÍ** | **Nabízená dodávka splňuje (ANO x NE)** |
| * Wifi controller integrovaný do NGFW platformy
 |  |
| * Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním
 |  |
| * Podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru
 |  |
| * Podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru
 |  |
| * Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení
 |  |
| * Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor)
 |  |
| * On-wire rogue AP detekce a mitigace
 |  |
| * Podpora fast-roamingu (802.11 k,v,r)
 |  |
| * Podpora více PSK u jednoho SSID
 |  |
| * Podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
 |  |
| Podpora WPA3 šifrování |  |

|  |  |
| --- | --- |
| **Základní technické požadavky****VIRTUALIZACE** | **Nabízená dodávka splňuje (ANO x NE)** |
| * Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext 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 kontext je zároveň samostatným wifi controllerem.
 |  |
| Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů). |  |

|  |  |
| --- | --- |
| **Základní technické požadavky****MANAGEMENT** | **Nabízená dodávka splňuje (ANO x NE)** |
| * 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.
 |  |
| * 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). |  |

**Konkrétní typ a označení nabízeného (HW i SW) řešení:** [DODAVATEL JEDNOZNAČNĚ URČÍ, JAKÝ TYP NEBO VERZE HW NEBO SW NABÍZENÉHO ŘEŠENÍ JE PŘEDMĚTEM JEHO NABÍDKY].

|  |  |
| --- | --- |
| **POŽADAVKY NA SLUŽBY SOUVISEJÍCÍ S DODÁVKOU NG FIREWALLŮ** | **Nabízená dodávka splňuje (ANO x NE)** |
| * Instalace a konfigurace NG firewall
 |  |
| * Migrace pravidel ze stávajícího firewallu (FortiGate 100F)
 |  |
| * Konsolidace a revize pravidel
* Revize oprávnění pro vzdálené přístupy
 |  |
| * Instalace a konfigurace nástroje pro analýzu logů
 |  |
| * Konfigurace SSO
 |  |
| * Konfigurace SSL inspekce
 |  |
| * Konfigurace dvou-faktorového ověřování
 |  |