Příloha č. 1: Technická specifikace předmětu plnění – položkový rozpočet

**Firewall**

**Počet ks: 2**

Ústav zemědělské ekonomiky a informací požaduje dodávku 2 zařízení firewall, které budou pracovat v HA módu Active-Pasive. Součástí dodávky bude kromě samotného zařízení (vč. redundantního zdroje):

záruka, podpora, kompletní implementace, migrace pravidel ze stávajícího firewallu a zaškolení dle požadavků uvedených dále.

Firewall musí obsluhovat (ovládat přímo z firewallu) stávající síťová zařízení: 26 ks AP (FAP223E a FAP221C), dále firewall spojuje tři odloučené pobočky IpSec šifrováním s Fortigate 40F. Tyto síťové zařízení zůstanou součástí nového řešení Firewallů.

Dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let pro všechny požadované bezpečnostní a síťové funkce. Pokud navrhované řešení využívá licence pro škálování výkonnosti, tak součástí plnění musí být licence splňující všechny výkonové požadavky od dodávky po dobu minimálně 5 let. V případě, že dosažení požadované výkonnosti vyžaduje doplnit řešení a jakýkoliv typ HW akceleračního modulu, tak tento modul musí být součástí dodávky. Součástí dodávky také musí být přímá technická podpora výrobce (zadavatel musí mít přímý kontakt na centrum technické podpory výrobce) na stejnou dobu, a to v režimu 24x7. Žádné z nabízených řešení nesmí být v době dodání zboží v režimu end of sales/end of support. Všechny požadované funkce musí být v době dodání zboží součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

Funkcionality povinné:

Kombinace funkcionalit IPS / IDS, síťové bezpečnostní funkce ochrana před sofistikovanými hrozbami, Deep Packet Inspection, Advanced Threat Protection - specifikovat co FW umí (Application Control, Intrusion Prevention, Web Filtering, Antivirus, Antispam, Cloud Sandbox).

|  |  |  |
| --- | --- | --- |
| Model – typové/výrobní označení: | [doplní dodavatel] | |
| Výrobce: | [doplní dodavatel] | |
| Parametr | Požadavek zadavatele | ANO / Lepší parametry |
|  | 2 redundantní zdroje 230V | [doplní dodavatel] |
|  | Napájecí kabely C13/14 k zapojení do PDU i do standardní sítě 230V | [doplní dodavatel] |
|  | WAN port minimálně rychlost 1Gb | [doplní dodavatel] |
|  | Min. 4x SPF port optického síťového rozhraní | [doplní dodavatel] |
|  | Min. 4x SPF+ porty optického síťového rozhraní | [doplní dodavatel] |
|  | 4x metalický 1Gb port | [doplní dodavatel] |
|  | Firewall musí být dodán jako funkční celek složený z komponent jednoho výrobce, a to včetně všech poskytovaných funkcionalit (např. typu IPS, AV, AS signatur | [doplní dodavatel] |
|  | databází pro URL kategorizaci, sandbox definic, případně dalších). | [doplní dodavatel] |
|  | Výrobcem musí být zajištěna na dodané FW podpora minimálně po dobu plánované životnosti/udržitelnosti 5 let od data dodání. | [doplní dodavatel] |
|  | FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů. | [doplní dodavatel] |
|  | FW musí být typu HW appliance. | [doplní dodavatel] |
|  | FW musí být kompatibilní s 19“ rozvaděčem. | [doplní dodavatel] |
|  | FW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k  CLI. | [doplní dodavatel] |
|  | FW musí obsahovat minimálně 4 SFP datové porty pro připojení k internetovým  routerům rychlosti min. 1 Gbps. | [doplní dodavatel] |
|  | FW musí obsahovat minimálně 4 SFP+ datové porty pro připojení k interním L2/l3  switchům rychlosti min. 10 Gbps. | [doplní dodavatel] |
|  | FW musí obsahovat minimálně 4x metalický port rychlosti 1Gbps. | [doplní dodavatel] |
|  | FW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW. | [doplní dodavatel] |
|  | FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP). | [doplní dodavatel] |
|  | FW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V. | [doplní dodavatel] |
|  | FW musí podporovat režim HA v módu Active – Active a Active- Pasive složený ze dvou a více zařízení. | [doplní dodavatel] |
|  | V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes FW. | [doplní dodavatel] |
|  | FW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy. | [doplní dodavatel] |
|  | Parametry propustnosti musí dodavatel uvádět v real world mix paketech, tzv. "application mix". | [doplní dodavatel] |
|  | Rychlost routování (stavový firewall) min. požadavek 25 Gbps (uveďte hodnotu). | [doplní dodavatel] |
|  | Propustnost firewallu při plné aplikační (application mix) kontrole musí dosahovat hodnoty minimálně 10 Gbps (uveďte hodnotu). | [doplní dodavatel] |
|  | Propustnost firewallu při plné aplikační kontrole (application mix) a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty minimálně 3 Gbps (uveďte hodnotu). | [doplní dodavatel] |
|  | Minimální počet naráz otevřených spojení musí dosahovat hodnoty alespoň 3 miliony (uveďte hodnotu). | [doplní dodavatel] |
|  | Zadavatel vyžaduje přítomnost Hw akcelerace přímo v zařízení. SW akcelerace výkonu je nepřípustná. | [doplní dodavatel] |
|  | FW musí plně podporovat IPv4 i IPv6. | [doplní dodavatel] |
|  | FW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3,  transparent. | [doplní dodavatel] |
|  | FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64. | [doplní dodavatel] |
|  | FW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding). | [doplní dodavatel] |
|  | PBF musí být možno nakonfigurovat na základě všech dostupných metrik alespoň typu interface, IP adresa. | [doplní dodavatel] |
|  | FW musí podporovat site-to-site VPN pomocí protokolu IPSec. | [doplní dodavatel] |
|  | FW musí podporovat remote access VPN pro uživatelská připojení pomocí  protokolů SSL (TLS). | [doplní dodavatel] |
|  | Propustnost IPSec musí být minimálně 10 Gbps. (uveďte hodnotu) | [doplní dodavatel] |
|  | Propustnost SSL-VPN musí být min. 2Gbps (uveďte hodnotu) | [doplní dodavatel] |
|  | FW musí podporovat multifaktorovou autentizaci pro VPN, OTP nebo FIDO nebo Microsoft proxy apllication | [doplní dodavatel] |
|  | SSL nebo L2TP nebo OpenVPN pro uživatelské připojení | [doplní dodavatel] |
|  | FW musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat  šifrování. | [doplní dodavatel] |
|  | FW musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu, bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí  podporovat šifrování | [doplní dodavatel] |
|  | FW musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash  disku. | [doplní dodavatel] |
|  | FW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius a osobní certifikát. | [doplní dodavatel] |
|  | FW musí obsahovat nativní nástroje pro debugging v úrovni L2 – L7 ISO/OSI modelu. | [doplní dodavatel] |
|  | FW musí podporovat nativní nástroj pro odchycení provozu. | [doplní dodavatel] |
|  | FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem. | [doplní dodavatel] |
|  | FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu. | [doplní dodavatel] |
|  | Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla. | [doplní dodavatel] |
|  | Definovaná aplikace musí představovat "match kritérium" při policy lookup. | [doplní dodavatel] |
|  | FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly. | [doplní dodavatel] |
|  | FW musí podporovat identifikaci aplikací na nestandardních portech. | [doplní dodavatel] |
|  | FW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | [doplní dodavatel] |
|  | FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských  identit. | [doplní dodavatel] |
|  | Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla. | [doplní dodavatel] |
|  | Uživatelská identita musí představovat "match kritérium" při policy lookup. | [doplní dodavatel] |
|  | FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – whitelisting pouze povolených aplikací a zákaz všeho ostatního, včetně neznámého  provozu. | [doplní dodavatel] |
|  | FW musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla. | [doplní dodavatel] |
|  | FW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | [doplní dodavatel] |
|  | FW musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla. | [doplní dodavatel] |
|  | FW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci. | [doplní dodavatel] |
|  | FW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů. FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto  dynamických seznamů. | [doplní dodavatel] |
|  | FW musí pro přístup ke kritickým aplikacím, poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci. Tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla. | [doplní dodavatel] |
|  | FW musí umožnit rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase. | [doplní dodavatel] |
|  | FW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a  aplikace. | [doplní dodavatel] |
|  | FW musí poskytovat možnost omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu +  čas apod.). | [doplní dodavatel] |
|  | FW musí podporovat prioritizaci provozu na základě DSCP. | [doplní dodavatel] |
|  | FW musí podporovat prioritizaci provozu na základě Identifikované aplikace. | [doplní dodavatel] |
|  | FW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému  mimo GUI. | [doplní dodavatel] |
|  | FW musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL. | [doplní dodavatel] |
|  | FW musí podporovat přeposílání logů ve formátu Syslog na zařízení třetích stran. | [doplní dodavatel] |
|  | Ukládání logů do interního úložiště o kapacitě minimálně 450GB | [doplní dodavatel] |
|  | Zasílání Logů na externí Syslog server | [doplní dodavatel] |
|  | Návrhne a zapojení FW do současné síťové infrastruktury. | [doplní dodavatel] |
|  | Součástí implementace je „hardening“ firewallu do nejvyššího možného zabezpečení s ohledem na nenarušení provozu. | [doplní dodavatel] |
|  | Součástí implementace je vyladění falešných pozitiv systému Threat Prevention, jako je IPS apod. | [doplní dodavatel] |
|  | Dodavatel zpracuje dokumentaci konfigurace a zapojení FW do síťové infrastruktury, včetně předané zálohy implementované konfigurace. | [doplní dodavatel] |
|  | Veškeré instalační a konfigurační práce budou provedeny osobou s prokazatelnou znalostí a zkušeností na dodávané řešení. | [doplní dodavatel] |
|  | Web filtering user activity - proxy server kontrolu provozu z LAN do WAN možnost i Antivirů, pro HTTP, HTTPS | [doplní dodavatel] |
|  | "SSL break and inspection" funkcionality | [doplní dodavatel] |
|  | Karanténa pro kontrolu zařízení připojovaných z VPN | [doplní dodavatel] |
|  | Sandbox | [doplní dodavatel] |
|  | Application Control | [doplní dodavatel] |
|  | Virtualizovatelnost systému pro případ disaster recovery | [doplní dodavatel] |
|  | API rozhraní pro integraci s technologiemi třetích stran (SIEM, MSSP services), content vectoring & screening (zadavatel předpokládá budoucí integraci do připravovaného prostředí integrovaného řízení bezpečnostních technologií (Managed Incident Response Systems+Managed Threat Protection Systems) | [doplní dodavatel] |
|  | MFA - OTP nebo FIDO pro VPN, Microsoft Entra application proxy | [doplní dodavatel] |
|  | Generování Netflow | [doplní dodavatel] |
|  | Zasílání Logů na externí Syslog server | [doplní dodavatel] |
|  | Email alerting | [doplní dodavatel] |
|  | MFA - OTP nebo FIDO pro VPN, Microsoft Entra application proxy | [doplní dodavatel] |
|  | WAF alespoň základní funkcionalita | [doplní dodavatel] |
|  | Wi-Fi kontroler | [doplní dodavatel] |
|  | AI-based Inline Malware Prevention | [doplní dodavatel] |
|  | Advanced Malware Protection | [doplní dodavatel] |
|  | URL, DNS & Video Filtering | [doplní dodavatel] |
|  | Antispam | [doplní dodavatel] |
|  | Attack Surface Security | [doplní dodavatel] |
|  | Napojení na interní LDAP server, Radius server | [doplní dodavatel] |
|  | Školení správců FW formou workshopu u zadavatele v rozsahu minimálně 3 dnů pro 2-3 osoby. | [doplní dodavatel] |
|  | Veškeré dodané zařízení musí být nové, nepoužité, určeno pro český trh, u výrobce zaregistrované na Zadavatele. Registraci musí být možné ověřit po zadání sériového čísla na www stránkách výrobce. | [doplní dodavatel] |
| Záruka a technická podpora | Podpora řešení problémů s provozem firewallu (nikoli jen výměna hw) na dobu 60 měsíců od data dodání bude poskytována v režimu 24/7. | [doplní dodavatel] |
| Technická podpora HW FW na dobu 60 měsíců od data dodání bude poskytována v režimu NBD (Next Business Day), tzn. odstranění nahlášené závady do druhého pracovního dne | [doplní dodavatel] |
| Technická podpora bude dodavatelem poskytována v českém jazyce. Dodavatel zajistí eskalaci na technickou podporu. | [doplní dodavatel] |