# Příloha č. 1

# Technická specifikace zboží

## Název/typ nabízených zařízení: Fortìgate FG-200F

Jsou požadována **2 zařízení Firewall** (vč. redundantního zdroje), které budou pracovat v HA módu Active-Active. Zařízení Firewall je určeno pro Národní zemědělské muzeum.

Zadavatel u zkoumaných možných řešení očekává využití takových produktových řad vybraných výrobků, u kterých výrobce a dodavatel zajistí podporu uvedených technologií v průběhu jejich životního cyklu pro nejméně polovinu jejich plánované životnosti.

**Požadavky na zařízení:**
**Porty:**

- WAN port minimálně rychlost 1Gb
- Min. 4x SPF port optického síťového rozhraní
- Min. 4x SPF+ porty optického síťového rozhraní
- 4x metalický 1GB port

**Podpora VPN:**

- VPN - IPSec pro Site-To-Site
- SSL nebo L2TP nebo OpenVPN pro uživatelské připojení

**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).

- Generování Netflow
- Zasílání Logů na externí Syslog server
- Email alerting
- Podpora řešení problémů s provozem firewallu, nikoli jen výměna hw, v České republice, případě Slovenské. Komunikace v českém jazyce
- MFA - OTP nebo FIDO pro VPN
- Napojení na interní LDAP server, Radius server
    - 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)

**Funkcionality volitelné:**

- Web filtering user activity - Proxy server kontrolu provozu z LAN do WAN možnost i Antivirů, pouze pro HTTP, HTTPS.
- "SSL break & inspection" funkcionality
- Karanténa pro kontrolu zařízení připojovaných z VPN
- Application Control
- Virtualizovatelnost systému pro případ disaster recovery

**Není požadováno:**

- WAF funkcionalita, bude řešeno samostatným HW
- Mailové funkcionality, ani mailové bezpečnostní
- Ochrana Wi-Fi nebo Wi-Fi kontrolery

**Dodavatel dále specifikuje**:

| **1. Základní požadavky** | ANO/NE/HODNOTA |
|---|---|
| Firewall musí být dodán jako funkční celek složený z komponent jednoho výrobce, a to včetně všech poskytovaných funkcionalit (např. typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic, případně dalších). | ANO |
| Výrobcem musí být zajištěna na dodané FW podpora minimálně po dobu plánované životnosti/udržitelnosti 5 let od data dodání. | ANO |
| FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů a uživatelů. | ANO |
| FW musí umožňovat navýšení výkonu přidáním další appliance. | ANO |
| **2. HW požadavky** | |
| FW musí být typu HW appliance. | ANO |
| FW musí být kompatibilní s 19“ rozvaděčem. | ANO |
| FW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI. | ANO |
| FW musí obsahovat minimálně 4 SFP datové porty pro připojení k internetovým routerům rychlosti min. 1 Gbps. | ANO |
| FW musí obsahovat minimálně 4 SFP+ datové porty pro připojení k interním L2/l3 switchům rychlosti min. 10 Gbps. | ANO |
| FW musí obsahovat minimálně 2x metalický port rychlosti 1Gbps. | ANO |
| FW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW. | ANO |
| FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP). | ANO |
| FW musí obsahovat dva nezávislé redundantní zdroje napájení AC 230V. | ANO |
| | |
| **3. High Availability (HA)** | |
| FW musí podporovat režim HA v módu Active – Active a Active- Pasive složený ze dvou a více zařízení. | ANO |
| 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. | ANO |
| FW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy. | ANO |
| **4. Výkonové parametry** | |
| Parametry propustnosti musí dodavatel uvádět v real world mix paketech, tzv. "application mix". | |
| Rychlost routování (stavový firewall) min. požadavek 25 Gbps (uveďte hodnotu). | 27 Gbps |
| Propustnost firewallu při plné aplikační (application mix) kontrole musí dosahovat hodnoty minimálně 10 Gbps (uveďte hodnotu). | 13 Gbps |
| Propustnost firewallu při plné aplikační kontrole (application mix) a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty minimálně 3 Gbps (uveďte hodnotu). | 3.5 Gbps |

| | |
|---|---|
| Minimální počet naráz otevřených spojení musí dosahovat hodnoty alespoň 3 miliony (uveďte hodnotu). | 3 Million |
| **5. Síťová funkcionalita** | |
| FW musí plně podporovat IPv4 i IPv6. | ANO |
| FW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent. | ANO |
| FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64. | ANO |
| FW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding). | ANO |
| PBF musí být možno nakonfigurovat na základě všech dostupných metrik alespoň typu interface, IP adresa. | ANO |
| **6. VPN** | |
| FW musí podporovat site-to-site VPN pomocí protokolu IPSec. | ANO |
| FW musí podporovat remote access VPN pro uživatelská připojení pomocí protokolů SSL (TLS). | ANO |
| Propustnost IPSec musí být minimálně 10 Gbps. (uveďte hodnotu) | 13 Gbps |
| Propustnost SSL-VPN musí být min. 2Gbps (uveďte hodnotu) | 2 Gbps |
| FW musí podporovat multifaktorovou autentizaci pro VPN, OTP nebo FIDO | ANO |
| **7. Management** | |
| FW musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování. | ANO |
| FW musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu, bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování | ANO |
| FW musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash disku. | ANO |
| FW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius a osobní certifikát. | ANO |
| FW musí obsahovat nativní nástroje pro debugging v úrovni L2 – L7 ISO/OSI modelu. | ANO |
| FW musí podporovat nativní nástroj pro odchycení provozu. | ANO |
| FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem. | ANO |
| **8. Aplikační kontrola** | |
| FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu. | ANO |
| Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla. | ANO |
| Definovaná aplikace musí představovat "match kritérium" při policy lookup. | ANO |
| FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly. | ANO |
| FW musí podporovat identifikaci aplikací na nestandardních portech. | ANO |
| FW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | ANO |
| **9. Kontrola uživatelské identity** | |
| FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit. | ANO |
| Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla. | ANO |

| | |
|---|---|
| Uživatelská identita musí představovat "match kritérium" při policy lookup. | ANO |
| **11. Bezpečnostní funkcionality** | |
| FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – whitelisting pouze povolených aplikací a zákaz všeho ostatního, včetně neznámého provozu. | ANO |
| 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. | ANO |
| FW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | ANO |
| 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. | ANO |
| FW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci. | ANO |
| FW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů. FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů. | ANO |
| 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. | ANO |
| FW musí umožnit rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase. | ANO |
| **12. AntiDDoS** | |
| 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. | ANO |
| **13. QoS** | |
| 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.). | ANO |
| FW musí podporovat prioritizaci provozu na základě DSCP. | ANO |
| FW musí podporovat prioritizaci provozu na základě Identifikované aplikace. | ANO |
| **14. Logování** | |
| FW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI. | ANO |
| 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. | ANO |
| FW musí podporovat přeposílání logů ve formátu Syslog na zařízení třetích stran. | ANO |
| **15. Migrace, konfigurace, nasazení do provozu** | |
| Návrh zapojení FW do současné síťové infrastruktury. | ANO |
| Součástí implementace je „hardening“ firewallu do nejvyššího možného zabezpečení s ohledem na nenarušení provozu. | ANO |
| Součástí implementace je vyladění falešných pozitiv systému Threat Prevention, jako je IPS apod. | ANO |

| | |
|---|---|
| Dodavatel zpracuje dokumentaci konfigurace a zapojení FW do síťové infrastruktury, včetně předané zálohy implementované konfigurace. | ANO |
| Veškeré instalační a konfigurační práce budou provedeny osobou s prokazatelnou znalostí a zkušeností na dodávané řešení. | ANO |
| **16. Nepovinné funkce** | |
| Specifikujte možnosti, které vámi uvedená nepovinná funkcionalita nabízí | |
| Web filtering user activity - proxy server kontrolu provozu z LAN do WAN možnost i Antivirů, pouze pro HTTP, HTTPS | ANO všechny |
| "SSL break and inspection" funkcionality | ANO |
| Karanténa pro kontrolu zařízení připojovaných z VPN | EMS |
| Sandbox | CLOUDová služba nebo HWNM appfiance |
| Application Control | ANO |
| Virtualizovatelnost systému pro případ disaster recovery | ANO |
| **17. Podpora** | |
| Podpora řešení problémů s provozem firewallu (nikoli jen výměna hw) na dobu 60 měsíců od data dodání bude poskytována v režimu 24/7. | ANO, Podpora, včetně evidence požadavků a řešení bude zajištěna prostřednictvím aplikačního portálu Prodejce na adrese https://xr.elat.cz |
| 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 | ANO |
| Technická podpora L1 bude dodavatelem poskytována v českém jazyce. Dodavatel zajistí eskalaci na technickou podporu L2, L3. | ANO |
| **18. Školení** | |
| Školení správců FW formou workshopu u zadavatele v rozsahu minimálně 3 dnů pro 2-3 osoby. | ANO |
| Školení bude vedeno autorizovaným instruktorem, nebo autorizovaným školícím centrem. | ANO |