



Služby bezpečnosti siete LAN

I.D.: 106770531

Prílohy:

- Zapisnica_vyhodnotenie_firewall.pdf (Pre zobrazenie príloh [testujte tu](#))
- sprava_o_zakazke_firewall.pdf (Pre zobrazenie príloh [testujte tu](#))
- LYNX_ponuka_Redigované.pdf (Pre zobrazenie príloh [testujte tu](#))
- Rámcová dohoda č. 344-2024-UVLF_5450015.pdf (Pre zobrazenie príloh [testujte tu](#))
- Príloha č. 2_5450018.pdf (Pre zobrazenie príloh [testujte tu](#))

Druh zákazky	Služby	Dátum publikovania	11.12.24
Typ oznámenia:	Výsledok	CPV kódy	72700000-7

Opis: Predmetom zákazky bolo poskytnutie komplexnej služby, ktorá zahŕňa široké spektrum činností zameraných na aktualizáciu, konfiguráciu, optimalizáciu a zabezpečenie bezpečnostných a sieťových komponentov v rámci UVLF. Cieľom je zvýšiť bezpečnosť, efektívnosť a odolnosť sieťovej infraštruktúry, pričom sa kladie dôraz na ladenie firewall pravidiel existujúcich technológií od výrobcu Fortinet, aktualizácie a rozšírenia kapacít existujúcej logovacej platformy FortiAnalyzer, podrobnú analýzu a optimalizáciu prebiehajúcej sieťovej komunikácie medzi servermi a pracovnými stanicami, ako aj migráciu Guest firewallu z Juniper na samostatnú VDOM na FortiGate Perimeter-FW. K tomuto účelu je tiež potrebné zabezpečiť dodávku a kompletnú integráciu vonkajších bezdrôtových prístupových staníc pre rozsiahle sieťové pokrytie, čo zahŕňa jej inštaláciu, konfiguráciu a testovanie v teréne, aby bola zabezpečená spoľahlivá a neprerušovaná konektivita v rámci celého areálu UVLF. Cieľom zákazky je nielen zvýšenie bezpečnosti prostredníctvom aktualizácií a optimalizácie, ale aj zabezpečenie vysokej dostupnosti a efektivity sieťovej infraštruktúry prostredníctvom pokročilých analytických a monitorovacích nástrojov. Taktiež sa kladie dôraz na minimalizáciu prerušenia služieb a zabezpečenie plynulej migrácie a integrácie nových komponentov do existujúcej sieťovej architektúry. Z uvedeného dôvodu požadoval verejný obstarávateľ implementáciu proxy servera, ktorý predstavuje bezpečnostné riešenie určené na ochranu prostredia pred webovými hrozbami a taktiež na zabezpečenie bezpečného prístupu k internetu, pričom musí poskytovať robustné možnosti filtrovania obsahu, kontroly prístupu a ochrany proti malvéru pre prichádzajúcu a odchádzajúcu webovú komunikáciu. Zákazka špecificky adresuje potreby v oblasti aktualizácie a rozšírenia technologických komponentov, optimalizácie sieťových pravidiel a konfigurácií pre zlepšenú bezpečnosť a efektívnosť. Zahŕnuté sú tiež činnosti súvisiace s analýzou a ladením komunikácie medzi rôznymi segmentmi siete, vrátane serverov a pracovných staníc, s cieľom identifikovať a eliminovať potenciálne slabiny a zvýšiť celkovú odolnosť proti kybernetickým hrozbám.