A meglévő határvédelmi rendszer bővítése és SCADA védelem kialakítása – Elvárások és követelmények

1. Bevezetés

A szervezetünk informatikai infrastruktúrájának egyik **legkritikusabb eleme a határvédelmi rendszer**, amely elsődleges szerepet tölt be az internet irányú forgalom biztonságos kezelésében. Ez a rendszer biztosítja az üzleti működés szempontjából elengedhetetlen szolgáltatásokat, mint az internetelérés, e-mail kommunikáció, VPN kapcsolatok, valamint a különböző külső interfészek – például az online ügyfélszolgálat, mobilalkalmazások és egyéb webes szolgáltatások – zavartalan működését.

Tekintettel arra, hogy ezek a szolgáltatások üzletkritikusak, a **határvédelmi rendszer esetleges meghibásodása vagy kiesése súlyos működési zavarokat okozhat**, amelyek közvetlen hatással vannak az ügyfélélményre, a belső folyamatokra és a szervezet külső megítélésére. Ezért kiemelten fontos, hogy a **rendszer redundáns módon kerüljön kialakításra**, biztosítva a folyamatos rendelkezésre állást, a hibatűrést és a gyors helyreállítást.

A jelen dokumentum célja, hogy meghatározza azokat az elvárásokat és keretfeltételeket, amelyek mentén a meglévő határvédelmi rendszerünk bővítése és redundáns kialakítása megvalósítható.

2. Célok

A tervezett fejlesztés keretében nemcsak a **meglévő határvédelmi rendszer redundanciáját** kívánjuk biztosítani, hanem egy **SCADA védelem kialakítását** is célul tűztük ki. Ezáltal lehetőség nyílik az informatikai rendszerünk felügyeleti és vezérlési komponenseinek fokozott védelmére, különös tekintettel az ipari és automatizált rendszerek biztonságára, amelyek egyre inkább integrálódnak a szervezet digitális működésébe.

Feladat a **Fortinet FortiGate-70F alapú, Active–Passive HA tűzfalmegoldás bevezetése**, kiegészítve FortiGuard UTP előfizetéssel, OT/SCADA biztonsági szolgáltatással és 100 felhasználós kétfaktoros hitelesítéssel. A cél a hálózati szolgáltatás-kiesések üzleti kockázatának csökkentése, az ipari rendszerek célzott védelme, valamint a hozzáférési kockázatok mérséklése.

3. Műszaki követelmények

Két darab FortiGate 70F (1 meglévő + 1 új) Active–Passive HA klaszterben kell üzemelnie. A FortiGate Clustering Protocol hiba vagy karbantartás esetén automatikus átállást hajtson végre a tartalék egységre, minimalizálva a kiesést. Az UTP előfizetés valós idejű fenyegetés intelligenciát és szignatúra frissítést kell biztosítson, az OT Security Service pedig ipari eszközökre és protokollokra szabott kontrollokkal egészíti ki a védelmet, illetve a 2FA mobil tokenek a felhasználói belépéseket védik.

a) A megoldás tartalma

- Hardver: FortiGate 70F tűzfalpár (HA), (1 meglévő és 1 új tűzfal)
- Szoftver/szolgáltatás: FortiCare Premium és FortiGuard UTP 3 éves opcióban (IPS, AMP/AV, App Control, URL/DNS/Video Filtering, Antispam).
- FortiGuard OT Security Service 2 licencben (új és meglévő egységre) 3 éves opcióval.
- FortiToken Mobile FTM ELIC 100 (100 felhasználó).

cikkszám	megnevezés	mennyiség
FG-70F	FortiGate-70F 10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port)	1
FC-10-0070F-950-02-36	FortiGate-70F 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2
FC-10-0070F-159-02-36	FortiGate-70F 3 Year FortiGuard OT Security Service (OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules)	2
FTM-ELIC-100	FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 100 users. Electronic license certificate. License transfer between devices is not allowed.	1

b) Implementáció

- Előkészítés: fizikai beépítés, illetve a teljekörű előkészítés. (ajánlatkérő feladata)
- Firmware-előkészítés: támogatott verzió kiválasztása és előkészítése.
- HA kialakítás: a másodlagos eszköz konfigurálása a kapott konfiguráció alapján.
- Beüzemelés karbantartási ablakban: klaszter felállítása, szinkronizáció ellenőrzése.
- Tesztelés: tesztek elvégzése (failover, elérések, stb) illetve komplett tesztelési jegyzőkönyv készítés.
- Dokumentáció: HA kialakítás komplett leírásának elkészítése
- A folyamatos üzemeltetési támogatás (monitoring, változáskezelés, on call) nem része a feladatnak.

c) Meglévő eszköz paraméterei

1 db FortiGate-70F 10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port)

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Advanced HW	2023-06-01	2028-05-30
Firmware & General Updates	Web/Online	2023-06-01	2028-05-30
Enhanced Support	Premium	2023-06-01	2028-05-30
Telephone Support	Premium	2023-06-01	2028-05-30
Advanced Malware Protection	Web/Online	2023-06-01	2028-05-30
FortiGuard IPS Service	Web/Online	2023-06-01	2028-05-30
FortiGuard URL, DNS & Video Filtering Service	Web/Online	2023-06-01	2028-05-30
AntiSpam	Web/Online	2023-06-01	2028-05-30

4. Pénzügyi feltételek

- Az implementáció során **beépített eszközöket és licenceket, mint szolgáltatást kívánjuk igénybe venni 3 éves időtartamra.**
- Tekintve, hogy a meglévő saját tulajdonú eszköz és a szolgáltatásként beüzemelt eszköz licenc lejárata nagy valószínűséggel el fog térni a beüzemelendő új eszközhöz kapcsolódó licencekétől ezt időben szinkronba szükséges hozni. Az ajánlatban ezt opcióként kell feltüntetni és abban az esetben lehet megrendelni, ha az új, HA eszköz beüzemelésre és aktiválásra került, a végső egységes lejárati dátumokat ekkor lehet pontosan rögzíteni.