10. számú melléklet: CTRL Menedzselt határvédelem

1. Szolgáltatás meghatározása

A CTRL Menedzselt határvédelem szolgáltatás keretében Szolgáltató tulajdonában álló központi, rendszerrel menedzselt határvédelmi szolgáltatást nyújt az Ügyfél hálózatában. Az internetelérés határvédelméhez a Szolgáltató a menedzselt eszközt beszerzi, leszállítja és telepíti. A telepített eszköz a Szolgáltató tulajdonában marad. Szolgáltató ügyeleti rendszert biztosít az esetleges meghibásodások bejelentésének fogadására, valamint a rendszer hibáinak elhárítása.
A szolgáltatás igényre szabható, kombinált kiberbiztonsági havidíjas szolgáltatás. A szolgáltatás csomagszűrést, vírus- és spamvédelmet és behatolásvédelmet nyújt egyetlen szolgáltatási csomagban, melynek terjedelme különböző igényeknek megfelelő, rugalmasan bővíthető és nem igényel Ügyfél oldali üzemeltetési feladatokat, sem az Ügyfél saját felelősségi körébe tartozó hálózati eszközt. A szolgáltatás magas rendelkezésre állást biztosít a központi rendszerén, 99,9%-os rendelkezésre állással.

2. Szolgáltatáselemek

2.1 Az Ügyfélnél elhelyezett, átruházásra nem kerülő, Szolgáltató által menedzselt tűzfaleszközök

A szolgáltatás igénybevételének alapfeltétele egy tűzfaleszköz választása. A szolgáltatás a 2.2 pontban részletezett alapdíjas vagy különdíjas funkciókkal bővül.
A szolgáltatás nyújtását az Ügyfél telephelyén telepített, átruházásra nem kerülő, Szolgáltató által menedzselt tűzfal eszköz biztosítja. Ezen eszköz biztosítja az Ügyfél telephelyén a szolgáltatás átadási pontját, ehhez csatlakoztathatja saját lokális hálózatát.
Ügyfél saját hálózati eszközeit (switch/router stb.) a tűzfal belső (LAN) Ethernet portjaira kötheti. A szolgáltatás Ügyféllel egyeztetett konfigurációját és a szolgáltatás átadását biztosító portot a Műszaki adatbekérőben a felek közösen rögzítik. A konfigurációt ennek alapján Szolgáltató a központi rendszerében állítja be.

2.1.1 FortiGate-30G

Belépő szintű, asztali modell, integrált SD-WAN (Software Defined Wide Area Network) funkcióval.

2.1.2 FortiGate-50G

A 30G-hez hasonlóan ez is egy kompakt, ventilátor nélküli asztali eszköz, amelyet az SP5 ASIC[1] hajt, azonban nagyobb port-sűrűséget és magasabb teljesítményt kínál. Támogatja a modern SD-WAN és NGFW (Next-Generation Firewall, újgenerációs tűzfal) funkciókat, lehetővé téve a komplex biztonsági házirendek alkalmazását a hálózati sebesség csökkenése nélkül. A megnövelt áteresztőképesség biztosítja az alkalmazások hatékony kiszolgálása sávszélesség-igényes alkalmazásoknál is.

2.1.3 FortiGate-70G

Növelt teljesítményű asztali modell (High-end desktop), szintén az SP5 processzorra épül. Rendkívül magas fenyegetés-elhárítási teljesítmény jellemzi, miközben megőrzi a helytakarékos kialakítást. Több GE (Gigabit Ethernet) RJ45 porttal, valamint dedikált WAN és FortiLink[2] csatlakozási lehetőségekkel rendelkezik a rugalmas hálózati integrációhoz. Ideális választás nagyobb igényű fiókirodák számára, ahol elvárás a nagy sávszélességű, titkosított forgalom (SSL/TLS[3]) mélyreható ellenőrzése a hálózati áteresztőképesség fenntartása mellett.

2.1.4 FortiGate-120G

Ez a modell már rack-be szerelhető (1U) kivitelű[4], és az SP5 processzor technológiája alkalmassá teszi a közepes méretű vállalati hálózatok kiszolgálására. A portok tekintetében a hagyományos GE portok

---

[1] Az SP5: a Fortinet ötödik generációs biztonsági processzora, amely több mint 20 évnyi ASIC-fejlesztés eredménye. Az ASIC (Application-Specific Integrated Circuit): célhardver, amelyet egy adott feladatra optimalizálnak. Fő célja: a hálózati forgalom titkosítása, ellenőrzése és biztonsági szabályok alkalmazása extrém sebességgel, miközben csökkenti a késleltetést és az energiaigényt.

[2] A FortiLink a Fortinet által kifejlesztett speciális csatlakozási és menedzsment lehetőség, lehetővé teszi, hogy a FortiGate tűzfal közvetlenül vezérelje és menedzselje a FortiSwitch hálózati switcheket és FortiAP hozzáférési pontokat. Ezáltal a teljes hálózat egyetlen központi eszközön keresztül irányítható. A fortinet saját fejlesztésű protokollja, amely a FortiGate és FortiSwitch közötti kommunikációt biztosítja.

[3] SL (Secure Sockets Layer): titkosított kapcsolatot biztosít böngésző és webkiszolgáló között; TLS (Transport Layer Security): Az SSL továbbfejlesztett, szabványosított változata, amelyet az IETF (Internet Engineering Task Force) szabványosított.

[4] : Az eszköz kialakítása megfelel az IEC szabványos 19 hüvelykes rack szekrény méreteinek, így könnyen beépíthető adatközponti vagy hálózati szekrénybe. 1U: A „U" (Unit) a rack magassági mértékegysége, így 1U = 1,75 hüvelyk ≈ 44,45 mm magas helyet foglal el a rack szekrényben.

mellett 10GE SFP+ uplink[5] csatlakozókkal is rendelkezik a gyorsabb gerinchálózati kapcsolat érdekében. Lehetővé teszi a nagy teljesítményű NGFW és SD-WAN kiszolgálást, valamint biztosítja a biztonságos hálózati konvergenciát és a felhőalapú alkalmazások gyors elérését.

2.1.5 FortiGate-200G

A középkategória egyik legerősebb tagja, amely szintén az SP5 ASIC-re épül, megnövelt teljesítmény biztosít a kisebb modellekhez képest. Rack-be szerelhető (1U), és gazdag port választékkal rendelkezik, beleértve a multi-gigabit és 10GE csatlakozókat. Kifejezetten a nagy forgalmú vállalati kampuszok igényeire szabták, ahol a belső szegmentálás és a titkosított forgalom valós idejű vizsgálata kritikus fontosságú. A modern hardver biztosítja, hogy a biztonsági szolgáltatások bekapcsolása biztosítsa a szükséges hálózati erőforrást.

2.1.6 FortiGate-400F

Ez a modell már a középvállalati szegmens felső részét célozza, nagy teljesítményű NP7 és CP9 processzorokkal[6]. Jelentős számú, hardveresen gyorsított 10GE SFP+ porttal rendelkezik, beleértve az ultra-alacsony késleltetésű (ULL) portokat is, amelyek speciális, időérzékeny alkalmazásokhoz (pl. tőzsdei kereskedés) ideálisak. 1U rack méretű, redundáns, üzem közben cserélhető tápegységekkel. Nagyvállalati környezetbe, adatközpontok peremvédelmére vagy belső hálózatok szegmentálására tervezték. A kiemelkedő teljesítmény lehetővé teszi a legszigorúbb biztonsági házirendek érvényesítését is anélkül, a hálózati teljesítmény szinten tartása mellett. A mesterséges intelligencián és gépi tanuláson alapuló FortiGuard szolgáltatásokkal kombinálva mélyreható védelmet és láthatóságot biztosít.

2.1.7 FortiGateRugged-60F

Speciális, ipari környezetre tervezett eszköz (OT). Strapabíró, ventilátor nélküli fémházzal rendelkezik, amely ellenáll a szélsőséges hőmérsékletnek, páratartalomnak és vibrációnak (IP20 vagy magasabb védettség). Hardveresen a 60F modellre épül, de rendelkezik speciális funkciókkal, mint például bypass port pár, amely áramkimaradás esetén is biztosítja a hálózati forgalom továbbítását, valamint soros portokkal ipari eszközök csatlakoztatásához. Olyan helyekre ideális, ahol a normál irodai környezettől eltérő, zordabb körülmények uralkodnak, például gyárakban, termelési üzemekben, közlekedési rendszerekben vagy kültéri telepítéseknél. Biztosítja a kritikus ipari vezérlőrendszerek (ICS/OT - Industrial Control Systems / Operational Technology) hálózatainak védelmét is a kibertámadásokkal szemben.

2.2 Alapszolgáltatásként alapdíjas és választhatóan igénybe vehető különdíjas szolgáltatási funkciók

2.2.1 ATP és UTP funkció-elemek

1. Alapfunkció (ATP): a Szolgáltatás alapértelmezett konfigurációjában az ATP (Advanced Threat Protection) funkció képezi. Ez magában foglalja hálózatbiztonsági és fájl alapú védelmi mechanizmusokat (ideértve a vírus- és kártevővédelmet).
2. Választható funkció (UTP): az UTP (Unified Threat Protection) funkció opcionálisan igényelhető, havidíjas elszámolású kiegészítő szolgáltatás. Az UTP funkció műszaki tartalma magában foglalja az ATP csomagban rögzített funkciókat, kiegészítve azokat Web és DNS szintű védelmi megoldásokkal (különös tekintettel a weboldalak kategorizált szűrésére és a levélszemét-szűrésre). Az UTP választása esetén az ATP szolgáltatás helyébe lép.

[5] 10GE = 10 Gigabit Ethernet, vagyis 10 Gbps adatátviteli sebességű; SFP+ (Small Form-Factor Pluggable Plus) = egy kisméretű, hot-swappable (üzem közben cserélhető) transceiver modul szabvány, amely támogatja a 10 Gbps sebességet; Uplink port = olyan port, amelyet tipikusan más hálózati eszközökhöz (pl. switch, router, szerver) való kapcsolódásra használnak, nem végfelhasználói eszközökhöz.

[6] A Fortinet NP7 hálózati processzor a Layer 2–4 hálózati rétegek feladatainak gyorsítását végzi, úgymint IP routing és NAT feldolgozás; IPsec VPN titkosítás; QoS és forgalomirányítás és DDoS elleni védelem (Host Protection Engine).
A Fortinet CP9 tartalomfeldolgozó processzor a biztonsági és tartalomellenőrzési feladatokat gyorsítja IPSec VPN motorként (akár 16 párhuzamos motor), elvégzi az SSL/TLS titkosítást és vizsgálatot, az IPS (Intrusion Prevention System) gyorsítását, valamint az alkalmazás- és tartalomszűrést.

Funkció-elemek	*ATP*	*UTP*	*Magyarázat*
			HÁLÓZATBIZTONSÁG
IPS (Intrusion Prevention System)	✓	✓	Hálózati behatolás-megelőző rendszer, amely valós időben elemzi az adatforgalmat, és automatikusan blokkolja az ismert biztonsági réseket kihasználó támadásokat, valamint a hálózati anomáliákat.
Malicious/Botnet URLs & IP reputáció	✓	✓	Botnetekhez kapcsolódó URL és IP blokkolása a rosszindulatú kommunikáció megelőzésére. Hálózati behatolás-megelőző rendszer, amely valós időben elemzi az adatforgalmat, és automatikusan blokkolja az ismert biztonsági réseket kihasználó támadásokat, valamint a hálózati anomáliákat.
			FÁJL TARTALMÚ VÉDELEM
Advanced Malware Protection (AMP)	✓	✓	Fejlett, többrétegű kártevő-elhárítási mechanizmus, amely a fájlok statikus vizsgálata mellett azok viselkedéselemzését is elvégzi a komplex fenyegetések detektálása érdekében.
Antivirus (AV)	✓	✓	Fejlett, többrétegű kártevő-elhárítási mechanizmus, amely a fájlok statikus vizsgálata mellett azok viselkedéselemzését is elvégzi a komplex fenyegetések detektálása érdekében.
Botnet Domains	✓	✓	A tartománynév-feloldás (DNS) szintjén működő védelem, amely automatikusan blokkolja a hozzáférést az ismert botnet hálózatokhoz köthető domain nevekhez.
Mobile Malware	✓	✓	Specifikus szűrőmechanizmus, amely a hálózati forgalomban detektálja és blokkolja kifejezetten a mobil operációs rendszereket (Android, iOS) célzó kártevőket.
Virus Outbreak Protection	✓	✓	Proaktív védelem, amely a globális fenyegetettségi adatok alapján azonnali védelmet nyújt a gyorsan terjedő új vírusvariánsok ellen, a végleges vírusdefiníciós adatbázis megérkezése előtti időszakban is.
Content Disarm & Reconstruct	✓	✓	Tartalom-helyreállítási technológia, amely a bejövő fájlokból eltávolítja az aktív, potenciálisan veszélyes kódokat (pl. makrók, beágyazott objektumok), és egy biztonságos, rekonstruált fájlmásolatot továbbít a végfelhasználónak.
AI-based Heuristic AV	✓	✓	Mesterséges intelligenciával támogatott heurisztikus elemzés, amely a kódstruktúra és viselkedési minták alapján képes azonosítani a még ismeretlen (zero-day) kártevőket.
FortiGate Cloud Sandbox / Sandbox SaaS	✓	✓	Mesterséges intelligenciával támogatott heurisztikus elemzés, amely a kódstruktúra és viselkedési minták alapján képes azonosítani a még ismeretlen (zero-day) kártevőket.
			WEB ÉS DNS VÉDELEM
URL Filtering	-	✓	Weboldalak kategorizálása és nem kívánt tartalom blokkolása böngészés közben. Kategória-alapú webes tartalomszűrés, amely lehetővé teszi a felhasználói hozzáférések szabályozását (engedélyezés, tiltás, naplózás) a weboldalak típusa és tartalma szerint (pl. szerencsejáték, felnőtt tartalom tiltása).
DNS Filtering	-	✓	DNS-protokoll szintű szűrés, amely megakadályozza a rosszindulatú, adathalász vagy a házirendnek nem megfelelő domain nevek feloldását, még titkosított webforgalom esetén is.
Video Filtering	-	✓	Videómegosztó platformokon (pl. YouTube) alkalmazható részletes tartalom-szabályozás, amely lehetővé teszi a videók elérésének korlátozását kategóriák, csatornák vagy egyedi azonosítók alapján.
Malicious Certificate	-	✓	Titkosított kapcsolatok ellenőrzése során a visszavont, lejárt, vagy ismert rosszindulatú forráshoz köthető SSL/TLS tanúsítványok automatikus blokkolása.

Funkció-elemek	*ATP*	*UTP*	*Magyarázat*
Anti-Spam	-	✓	A bejövő elektronikus levelezés szűrése az SMTP protokoll szintjén, amely kiszűri a kéretlen reklámleveleket (spam) és a rosszindulatú csatolmányokat vagy linkeket tartalmazó üzeneteket.
			SD-WAN
SD-WAN	✓	✓	Szoftveresen definiált nagy kiterjedésű hálózati (SD-WAN) technológia, amely intelligens, alkalmazás-alapú forgalomirányítást és terheléselosztást biztosít több WAN kapcsolat között a szolgáltatásfolytonosság érdekében.

2.3 Az ATP/UTP funkciókon túl választható különdíjas szolgáltatási funkciók

2.3.1 A FortiToken (MFA) választható funkció

Többfaktoros hitelesítést (MFA) biztosít a felhasználói azonosítás megerősítésére. A rendszer célja a jelszóalapú védelem kiegészítése egy második faktorral, így csökkentve a kompromittált hitelesítő adatokból eredő támadások kockázatát. A Szolgáltató által használt token típus az annak működése:

- **FortiToken Mobile**: OATH-kompatibilis alkalmazás iOS és Android platformokra, amely időalapú (TOTP) vagy eseményalapú (HOTP) egyszer használatos jelszavakat (OTP) generál, valamint támogatja a push értesítéses hitelesítést. A tokenmagok dinamikusan generálódnak, és titkosítva vannak tárolva és továbbítva.

2.3.1.1 Hitelesítési módok

- **OTP alapú MFA**: A felhasználó a jelszó megadása után egy egyszer használatos kódot ad meg, amelyet a FortiToken generál.
- **Push alapú MFA**: A felhasználó mobil eszközén megjelenő értesítésen keresztül hagyja jóvá vagy utasítja el a bejelentkezést. A push folyamat a Fortinet felhőszolgáltatásán (push.fortinet.com) keresztül kommunikál a mobileszköz értesítési infrastruktúrájával.

2.3.1.2 Integrációs és architektúra lehetőségek tokenes hitelesítés esetében

- **FortiGate integráció**: A FortiToken közvetlenül használható FortiGate NGFW eszközökkel VPN, adminisztrációs hozzáférés és captive portal MFA biztosítására.
- **FortiAuthenticator**: Központi RADIUS szerverként működik, amely kezeli a tokeneket és a felhasználói hitelesítést, valamint támogatja az API és LDAP integrációt.

2.3.1.3 Biztonsági jellemzők

- Titkosított tokenmagok: A token seed-ek mindig titkosítva vannak, mind nyugalmi állapotban, mind átvitel közben.
- Eszközhöz kötött tokenek: A mobil tokenek egyedi eszközhöz kötődnek, így megakadályozva a jogosulatlan másodlagos regisztrációt.

2.3.2 FortiGuard OT Security Service választható funkció

A FortiGate NGFW platformhoz kapcsolódó, előfizetéses licencen alapuló funkció, amely speciális IPS (Intrusion Prevention System) és Application Control funkciókat biztosít ipari és SCADA környezetekben. A cél az OT hálózatok és eszközök (pl. PLC, RTU, HMI) védelme az ipari protokollokra optimalizált fenyegetések ellen, valós idejű forgalomelemzéssel és támadásblokkolással.

2.3.2.1 Funkcionális komponensek

- **Ipari protokoll-támogatás**: Több száz OT-specifikus IPS és alkalmazásvezérlési aláírás (pl. Modbus, DNP3, IEC 61850) a protokollszintű forgalom azonosítására és szabályozására.
- **Deep Packet Inspection (DPI)**: Passzív csomagszintű elemzés az OT hálózati forgalom felett, amely képes detektálni és blokkolni a rosszindulatú aktivitást.
- **Virtuális patching**: Ismert és ismeretlen sebezhetőségek elleni védelem addig, amíg a gyártói javítás elérhetővé nem válik.

- **Automatikus frissítés**: A FortiGuard Labs fenyegetésintelligencia adatbázisából származó új IPS aláírások folyamatos letöltése és alkalmazása.

2.3.2.2 Architektúra és integráció

- **FortiGate NGFW**: Az OT Security Service a FortiGate tűzfal biztonsági profiljaiban (IPS, Application Control) aktiválható.
- **FortiManager és FortiAnalyzer:** Központosított menedzsment és naplóelemzés az OT biztonsági eseményekhez.

2.3.2.3 Biztonsági jellemzők

- **OT-specifikus IPS és alkalmazásvezérlés:** Több ezer szignatúra ipari alkalmazásokhoz és protokollokhoz.
- **Szabályozói megfelelés támogatása:** NIST CSF, IEC 62443 és más ipari szabványoknak megfelelő biztonsági kontroll biztosítása.
- **Valós idejű fenyegetésdetektálás:** Anomáliák és támadások azonnali blokkolása az OT hálózatban.
- **IT/OT konvergencia:** Egységes biztonsági architektúra a Fortinet Security Fabric részeként, amely lefedi az IT és OT környezeteket.

2.3.3 Fortinet SD-WAN

A szolgáltatásunk mindegyik tűzfaleszköze alkalmas és fel van készítve az SD-WAN (Software-Defined Wide Area Network) funkciók ellátására, amennyiben Ügyfél ezt a kiegészítő szolgáltatást választja. Ezek az eszközök nem csupán biztonsági (esetleges internet vonal redundancia), hanem hálózatoptimalizálási feladatokat is képesek ellátni. A biztonságközpontú hálózatépítés elve alapján, ahol az SD-WAN és az újgenerációs tűzfal (NGFW) képességek egyetlen könnyen menedzselhető eszközben képes nyújtani a szolgáltatás.

2.3.3.1 Igénybe vehető SD-WAN Képességek

Alkalmazásközpontú forgalomirányítás (Application Steering): a szolgáltatás tűzfaleszközei több ezer alkalmazást képesek azonosítani, és a forgalmukat dinamikusan a legmegfelelőbb WAN útvonalra irányítani (pl. MPLS, szélessávú internet, 4G/LTE). Ez biztosítja a kritikus üzleti alkalmazások, mint a SaaS szolgáltatások vagy az egységes kommunikációs platformok optimális működését.

Dinamikus útvonalválasztás és link-felügyelet (Dynamic Path Steering & Link Health Monitoring): a szolgáltatás tűzfaleszközei folyamatosan mérik a WAN kapcsolatok minőségét (késleltetés, jitter, csomagvesztés), és automatikusan átterelik a forgalmat egy jobban teljesítő kapcsolatra hiba vagy teljesítményromlás esetén.

Biztonságos SD-WAN: a biztonsági funkciók (NGFW, IPS, antivírus, webfilter) mélyen integráltak a szolgáltatásba, beleértve a teljes SD-WAN forgalmat, valamint a titkosított forgalmat is. Ez hatékony védelmet biztosít a kiberfenyegetésekkel szemben. A tűzfaleszközök igény esetén SSL-ellenőrzést tesznek lehetővé a WAN kapcsolatokon folyó forgalmakon.

Analitika és riportolás: a Szolgáltató valós idejű és historikus adatokat gyűjt a hálózati teljesítményéről és az anomáliákról, segítve a hibaelhárítást és a hálózat esetleges optimalizálását.

2.3.4 Rendszeres automatikus riportok

Automatikusan generált, ütemezett jelentések az eltelt időszak szolgáltatásáról (e-mailben elküldve ez ügyfél által megadott kapcsolattartási email címre, az SLA-melléklet szerint., PDF/xlsx formátumban):

2.3.4.1 Havi riport (a szolgáltatás alapbeállítása)

Részletes compliance, SLA teljesítés, kockázati trendek, ajánlások.

2.3.4.2 Heti riport (Különdíjas szolgáltatás)

Uptime %, top threat events, traffic summary, incidensek.

2.3.5 Eseti igénykezelés

2.3.5.1 Alap szolgáltatás részeként, abba beleértve
Műszakidőben (hétköznapokon, 9:00-17:00 között) ***havi 2 mérnökóra*** eseti igénykezelés (pl. kisebb config módosítás, konzultáció, riport elemzés). Felhasználható bármely hónapban, ticket-alapú elszámolással.

2.3.5.2 További igénykezelés (különdíjas)
Túlóra vagy műszakidőn kívüli igények (pl. emergency change, audit, extra kérések) külön megállapodással, eseti ajánlattal szerint megvalósítható. Ez jelen szolgáltatásnak ez nem része.

3. Szolgáltatás igénybevételének feltételei

- **Az Ügyfél által biztosítandók**
    - 230V-os áramellátás a szolgáltatás nyújtásához szükséges végponti tűzfaleszköz részére, annak üzemelési helyén (240Vac/0,6A, 35,3 W átlagos / 39,1 W max.).
    - Az eszközök üzemeltetéséhez szükséges hely (H/m x W/sz x L/h (mm) 44 x 432 x 254, központhelyiségben, szerverszobában, rack-szekrényben).
    - A pontos méret eszközönként:
        - FortiGate 30G esetében: 40.5 x 142 x 160 mm
        - FortiGate 50G esetében: 40.5 x 142 x 160 mm
        - FortiGate 70G esetében: 62 × 216 × 160 mm
        - FortiGate 120G esetében: 44 × 432 × 254 mm
        - FortiGate 200G esetében: 44 × 432 × 342 mm
        - FortiGate 400F esetében: 44,45 × 432 × 380 mm
    - FortiGate Rugged 60F esetében: 42.7 x 216 x 170 mm
    - Korlátlan hozzáférés a szolgáltatás nyújtásához szükséges eszközökhöz Szolgáltató számára, a rendelkezésre állásával egyező időintervallumokban (7x24 vagy 5x10 órában).
    - Az üzembiztos működéshez szükséges feltételek: hőmérséklet 0°–tól 40°C –ig, páratartalom: 10%-90%-os nem kondenzációs) megteremtése és fenntartása, szükség esetén klimatizálás (hőleadás: <125 BTU/h).
        - FortiGate 30G esetében: 46 BTU/h hőleadás
        - FortiGate 50G esetében: 47 BTU/h hőleadás
        - FortiGate 70G esetében: 80 BTU/h hőleadás
        - FortiGate 120G esetében: 159 BTU/h hőleadás
        - FortiGate 200G esetében: 342 BTU/h hőleadás
        - FortiGate 400F esetében: 645 BTU/h hőleadás
        - FortiGate Rugged 60F esetében: 72 BTU/h hőleadás
    - A végponti tűzfaleszköz elhelyezése során biztosítani kell Ügyfélnek a Szolgáltató számára, hogy a tűzfaleszköz az Ügyfél internet elérése és az internetelérést fogadó router közé kerülhessen.
    - Fenti feltételeket Ügyfél díjmentesen biztosítja a szolgáltatás nyújtásához.

4. A létesítés feltétele és határideje

4.1 Az Ügyfél által hiánytalanul kitöltött és Szolgáltató által visszaigazolt Műszaki adatbekérő megléte, mely az Egyedi Szolgáltatási Szerződés melléklete.

4.2 A Szolgáltató tűzfaleszköz(ök) Szolgáltató raktárába történő beérkezését követően, négy (4) héten belül a megkezdi a létesítést.

A szolgáltatás létesítettnek minősül, ha Szolgáltató Ügyfél telephelyén létesítette a Szolgáltató tulajdonában lévő tűzfaleszközt.

5. A munkavégzés részletes feltételei
A Szolgáltató feladatainak ellátásához – beleértve az implementációt és az üzemeltetés megkezdését is – az Ügyfél köteles az alábbi feltételeket biztosítani:

- a feladatellátásban érintett rendszerekhez és eszközökhöz szükséges **megfelelő jogosultságokat** (adminisztrátori / root szintű hozzáférés) a Szolgáltató i számára;
- az érintett eszközökhöz és rendszerekhez történő **fizikai és logikai hozzáférést**, beleértve a telephelyre, szerverszobába történő bejutást, valamint a virtuális környezetek elérését;
- **műszakilag kompetens kapcsolattartó személy(ek)** elérhetőségét a munkanapokon 9:00–17:00 óra között, akik jogosultak a konfigurációhoz szükséges hálózati és rendszeradatok (pl. IP-topológia, VLAN-struktúra, routing) egyeztetésére;
- az implementációhoz és a szolgáltatás nyújtásához a Műszaki adatbekérőben **meghatározott hálózati sávszélességet**, amely alkalmas a menedzsment-, adminisztrációs és monitorozási forgalom zavartalan lebonyolítására.

A Szolgáltató felelőssége nem terjed ki azon események, hibákra vagy következményekre, amelyek az Ügyfél vagy harmadik fél által, a Szolgáltatóval történő előzetes egyeztetés és jóváhagyás nélkül végrehajtott módosításokból vagy beavatkozásokból erednek azon rendszereiben, melyek más működést eredményeznek, mint amit az Műszaki adatbekérőben Szolgáltató és Ügyfél közösen rögzített.

6. Szolgáltatás díjazása

A szolgáltatás ellenértéket az Egyedi Szolgáltatási Szerződés tartalmazza.

7. Szolgáltatási szintek (SLA)

Szolgáltatási szint megnevezése	Szolgáltatási szint tartalma	Értéke
A gyártó által kibocsátott frissítések, javítások telepítése	Szolgáltató a gyártó által díjmentesen kibocsátott, az Ügyfél rendszere szempontjából releváns frissítéseket, biztonsági javításokat rendszeresen, a kockázatoknak és a sérülékenység súlyának megfelelő időtartamon belül telepíti. A frissítések ütemezése és végrehajtása a feltárt kockázatok, valamint a sérülékenységek súlyossági szintje alapján történik, a szolgáltatásbiztonság fenntartásának elsődleges figyelembevételével. A szolgáltatás nem foglalja magában a főverzióváltással járó rendszerfrissítéseket. A frissítési időszak nem számít bele a szolgáltatás rendelkezésre állási időbe.	A Szolgáltató a tervezett frissítésekről az Ügyfélt legalább 24 órával a végrehajtás előtt értesíti. Kritikus biztonsági sérülékenység esetén a frissítések soron kívül, rendkívüli karbantartás keretében is végrehajthatók.
Tervezett karbantartás	A Tervezett karbantartás nem számít bele a szolgáltatás rendelkezésre állási időbe. A karbantartás időpontja előzetesen emailben vagy a Service Desk rendszeren keresztül értesítve kerülnek ütemezésre.	7 munkanap
Hibaelhárítás rendelkezésre állása	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése esetén a hibaelhárítást az adott időszakra értelmezett szolgáltatásként biztosítja. A hibaelhárítás magában foglalja az incidens kivizsgálását, a hiba okának azonosítását, valamint a szolgáltatás működésének helyreállítására irányuló intézkedéseket.	Elérhetőség: 7×24 (napi 24 óra, heti 7 nap)
Manuális hibaelhárítás megkezdése	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése esetén a szerződésben szabályozott módon bejelentett, hibák esetén a hiba elhárítását legkésőbb az adott időn belül elkezdi, a hibaelhárítás rendelkezésre állási időtartamához igazodva.	A hibaelhárítás megkezdése a hiba jegy létrehozása után max. 4 órán belül.
Rendszeres riport, elemzés nélkül	Szolgáltató a riport sablon segítségével elkészíti a beszámolót, további elemzést az ebben látszó eseményekről nem folytat, nem ad konkrét javaslatokat. A riport kizárólag az összegyűjtött adatok és események bemutatását tartalmazza; a Szolgáltató a riportban szereplő eseményekhez kapcsolódóan **nem végez részletes elemzést, nem készít értelmezést, és nem fogalmaz meg konkrét biztonsági vagy konfigurációs javaslatokat**.	**heti / havi** riport a szerződés szerint

Szolgáltatási szint megnevezése	Szolgáltatási szint tartalma	Értéke
A központi rendszer éves rendelkezésre állása	A Szolgáltató vállalja, hogy a központi rendszer a naptári év során folyamatosan elérhető. A központi rendszer rendelkezésre állásának mértéke a naptári év teljes időtartamára vetítve kerül meghatározásra, a jelen szerződésben és az SLA-ban rögzített feltételek szerint. Naptári év: 365 nap.	99,9%

7.1 Az SLA alkalmazásának korlátjai

Nem számolandó a rendelkezésre állásba harmadik fél szolgáltató hibája miatt SLA sértés (különösen az internetszolgáltató által okozott szolgáltatáskimaradás), valamint a sürgős biztonsági beavatkozás miatt SLA sértés. Szolgáltató a sürgős biztonsági beavatkozásról – legkésőbb annak elvégzést követő 24 órán belül – értesíti Ügyfelet. A sürgős biztonsági beavatkozás célja a Szolgáltató infrastruktúrájának biztonsági, stabilitási vagy integritási fenyegetéseinek elhárítása (pl. DDoS támadás, zero-day sérülékenység, ransomware). A beavatkozásról részletes riport kerül kiadásra.

8. Szolgáltatás áthelyezése

- Amennyiben Ügyfél Szolgáltatótól a Szolgáltatás áthelyezését kéri egy fizikai telephelyéről egy másik, földrajzilag eltérő telephelyére, úgy az Ügyfél a Szolgáltatótól a **Szolgáltatás házon kívüli áthelyezés**ét kéri.
- Amennyiben Ügyfél Szolgáltatótól a Szolgáltatás áthelyezését kéri a Szolgáltatási végpont telephelyén belül, úgy Ügyfél a Szolgáltatótól a Szolgáltatás házon belüli **áthelyezését** kéri.
- Az új szolgáltatási végponton szükséges a szolgáltatás nyújtásához szükséges feltételeket Ügyfélnek biztosítani
- A szolgáltatás hozzáférési pont áthelyezésére – a szükséges műszaki feltételek fennállása esetén –, külön díjfizetési kötelezettség mellett nyílik lehetőség.

Szolgáltatás áthelyezés helyszíne	Az áthelyezési díj mértéke Megegyezik az igénybe vett szolgáltatáscsomag mindenkori:
Házon kívüli áthelyezése	**egyszeri havidíj**ával.
Házon belüli áthelyezése	**egyszeri havidíj 50%**-ával.

9. Szolgáltató az alábbi szolgáltatási csomagokat a továbbiakban nem értékesíti

9.1 Starter

A Starter előre beállított csomag- és webszűrést tartalmaz. Nem tartalmaz konfigurációs lehetőségeket, rendszeres riportokat, illetve riasztásokat.

A csomag tartalma:
Kezdeti beállítás (lásd a szolgáltatásra vonatkozó Adatbekérőt)
Tűzfal funkció, csomagszűrés

9.1.1 Tűzfal funkció, csomagszűrés

- Az Ügyféltől az internet irányába kezdeményezett minden szükséges kapcsolat engedélyezett.
- Az internet felől az Ügyfél belső hálózata felé irányuló kapcsolatkezdemények tiltottak. Ez alól az Ügyfél publikus szerverei (pl. webszerver), valamint a távmunkát lehetővé tevő VPN szervere felé irányuló kapcsolatok lehetnek kivételek.
- Az Ügyfél belső hálózati címei egyetlen NAT-olt IP-n jelennek meg a szolgáltatási pont felé. (Nincs lehetőség az Ügyfél alhálózatainak külön kezelésére.)

9.2 Basic

A Basic csomag tartalmazza a Starter csomag elemeit. Ezen felül előre meghatározott, testreszabott kibervédelmi funkciókat nyújt. A csomag az alábbiakat tartalmazza:

A Basic csomag tartalma
AWeb-tartalom szűrése (kártékony oldalak URL- és tartalmi kategória szerint)
Port alapú szűrés
Alkalmazás kontroll

9.2.1 Web-tartalom szűrés

- Kártékony weboldalak kiszűrése URL-kategória-alapon.
- Tartalmi kategórián alapuló szűrés: a szűrés során választható kategóriák (pl.: felnőtt tartalmak, játékoldalak) tiltása.

Fő Kategória	**Alkategória**
kötelezően tiltott	Gyermekbántalmazás (Child Abuse)
kötelezően tiltott	Diszkriminatív (Discrimination)
kötelezően tiltott	Drog és erőszak (Drug Abuse, Explicit Violence)
kötelezően tiltott	Extrém Csoportok (Extremist Groups)
kötelezően tiltott	Hacker oldalak (Hacking)
kötelezően tiltott	Illegális tartalmak (Illegal or Unethical)
kötelezően tiltott	Plagizáló tartalmak (Plagiarism)
kötelezően tiltott	Proxy elkerülő oldalak (Proxy Avoidance)
Felnőtt Tartalom	Szerencsejáték (Gambling)
Felnőtt Tartalom	Pornográf oldalak (Pornography)
Felnőtt Tartalom	Szex témájú oldalak (Nudity and Risque, Other Adult)
Felnőtt Tartalom	Fegyverek és sportvadászat (Sports hunting, Weapons)
Sávszélességet igénylő	Fájl megosztás / tárhely (File Sharing and Storage)
Sávszélességet igénylő	P2P fájl megosztás (Peer-to-Peer File Sharing)
Biztonsági kockázatott rejtő oldalak	Kártékony oldalak (Malicious Websites)
Biztonsági kockázatott rejtő oldalak	Adathalász oldalak (Phising)
Biztonsági kockázatott rejtő oldalak	Spam oldalak (Spam URLs)

- Sávszélességet erősen igénybe vevő szolgáltatások (pl.: streaming media, p2p, file sharing stb.) elérésének szűrése.

Biztonságos keresés (a keresőmotorok SafeSearch funkciójának) kikényszerítésével.

9.2.2 Port alapú szűrés

A tűzfalszabályok kialakítása Ügyfél egyedi igényei alapján (portszámok). A port szűrés a tűzfalak egyik alapvető funkciója, amely a hálózati forgalmat a használt TCP vagy UDP portszámok alapján engedélyezi vagy blokkolja, lehetővé téve, hogy csak a meghatározott szolgáltatások legyenek elérhetők, miközben minden más forgalom tiltásra kerül.

9.2.3 Alkalmazás kontroll

- Tiltásra kerülő alkalmazáskategóriák:

botnet
p2p
proxy

- Átengedésre kerülő alkalmazáskategóriák:

all other known applications
Gyártói adatbázisban még nem szereplő alkalmazás

9.3 Standard

A csomag tartalmazza mindazokat a szolgáltatási elemeket, amelyeket a Basic csomag, ezenfelül pedig havi rendszerességű riportokat, javaslatokat és heti szintű igénykezelési lehetőséget tartalmaz.
A Standard csomag a Basichez képest többek között malware szűrést tartalmaz. Ez a megoldás a szignatúra alapú védelmen túl valós idejű fájl vizsgálatot is végez a felhőben. A Standard csomag a Basic csomaghoz képest az alábbi elemekkel bővül:

Szolgáltatáselemek	**Rövid leírás**
Szabályrendszer finomhangolása	A tűzfalon ideális egyensúly fenntartása a sebesség és biztonság érdekében
Site-to-Site VPN (telephelyek közötti virtuális magánhálózat)	Titkosított kapcsolat létrehozása több, általában földrajzilag elkülönülő hálózat között
Malware (rosszindulatú kód, vírus) szűrése	Alapvető védelmi képességeket biztosít a mai kifinomult támadások ellen, védelmet nyújtva az ismert és ismeretlen fenyegetésekkel szemben
SPAM (kéretlen levelek) szűrése	A spamszűrő kéretlen, nem kívánt és fertőzött e-mailek felismerésére szolgál, továbbá megakadályozza, hogy ezek az üzenetek eljussanak a postaládába
Havi riport és konzultáció	Összefoglaló jelentés az eltelt időszakról, valamint ennek kiértékelése és közös áttekintése

9.4 Professional

A Professional a Standard csomag tartalmán felül napi szintű igénykezelési lehetőséget nyújt, emellett többek között heti riportokat, részletesebb behatolásvédelmet (IPS) és kliens VPN-t is biztosít. A kliens VPN biztonságos hozzáférést nyújt a vállalat belső hálózatához, legyen szó távmunkáról vagy időszakos távoli bejelentkezésekről.
A Professional csomag a Standard csomaghoz képest az alábbi elemekkel bővül:

Szolgáltatáselemek	**Rövid leírás**
Napi igénykezelés	Aktív mérnöki közreműködés a folyamatokban napi szinten
Heti automatikus riportok	Automatikus, ütemezett jelentés az eltelt időszakról
IPS (behatolásvédelem)	Az IPS (Intrusion Prevention System) behatolásgátló rendszer folyamatosan figyeli a hálózati forgalmat a fenyegetések azonosítása érdekében. Az IPS egyben behatolásmegelőző rendszer is
Kliens-VPN	Lehetővé teszi a felhasználók számára, hogy biztonságos, titkosított kapcsolatot hozzanak létre pl. a távmunkához
DNS-filter, tartománynevek szűrése	Blokkolja a rosszindulatú vagy tiltott webhelyeket és alkalmazásokat, így azok nem tölthetők be az eszközökön
QoS (szolgáltatásminőség)	Lehetővé teszi a hálózati forgalom szabályozását, priorizálását a kritikus alkalmazások teljesítményének biztosítása érdekében

9.5 Opcionális funkciók:

Az alapszolgáltatáson túl igényelhető további funkciók, amelyek az ügyfél igénye szerint aktiválhatók.

A csomagok részeit képező, valamint választható kiegészítő szolgáltatási elemek

Csomagok tartalma	Starter	Basic	Standard	Professional
Kezdeti beállítás	■	■	■	■
Csomagszűrő tűzfal	■	■	■	■
Web-tartalom szűrése (kártékony oldalak URL- és tartalmi kategória szerint)	■	■	■	■
Port alapú szűrés	▒	■	■	■
Alkalmazás kontroll (botnet, p2p, proxy, egyéb ismert és ismeretlen alkalmazások)	▒	■	■	■
Szabályrendszer finomhangolása	▒	▒	■	■
Site-to-Site VPN (telephelyek közötti virtuális magánhálózat)	▒	▒	■	■
Malware (rosszindulatú kód, vírus) szűrése	▒	▒	■	■
SPAM (kéretlen levelek) szűrése	▒	▒	■	■
Havi riport és konzultáció	▒	▒	■	■
Napi igénykezelés	▒	▒	▒	■
Heti automatikus riportok	▒	▒	▒	■
IPS (behatolásvédelem)	▒	▒	▒	■
Kliens-VPN	▒	▒	▒	■
DNS-filter, tartománynevek szűrése	▒	▒	▒	■
QoS (szolgáltatásminőség)	▒	▒	▒	■
Automatikus napi riport	▒	▒	▒	▒
APT (fejlett támadások) elleni védelem	▒	▒	▒	▒

A Szolgáltatáscsomagok igény szerint testre szabhatóak választható kiegészítő szolgáltatási elemekkel.

■ A csomagban foglalt szolgáltatási elem. ▒ A csomaghoz választható kiegészítő szolgáltatási elem.

A választható kiegészítő szolgáltatások **a szerződési évforduló alkalmával** módosíthatók.
Két választható szolgáltatási elem egyik csomag részét sem képezi, ugyanakkor mindegyik csomaghoz választható kiegészítő szolgáltatási elemként:

Szolgáltatáselemek	Rövid leírás
Automatikus napi riport	Automatikus, ütemezett jelentés az eltelt időszakról
APT (fejlett támadások) elleni védelem	Az APT (Advanced Persistent Threat) olyan támadásra utal, amellyel titokban és innovatív hacker módszerekkel hozzáférnek egy rendszerhez és ezt a hozzáférést hosszú ideig észrevétlenül kihasználják

10. Kapcsolattartás és Ügyfélszolgálat elérhetőségei

Kapcsolattartók	Név	Elérés
A Szolgáltató oldaláról (ügyfélszolgálat):	**Servicedesk**	Tel.: +36/80/40-80-80 Mail: servicedesk@telekom.hu Fax.: +36/1/432-8290

11. Adatvédelmi rendelkezések

A CTRL Menedzselt határvédelem szolgáltatással kapcsolatban a Szolgáltató (a továbbiakban: Adatfeldolgozó) az Ügyfél (a továbbiakban: Adatkezelő) adatfeldolgozójaként jár el az IÁSZF törzsrésze szerint.

A Szolgáltatás:	CTRL Menedzselt határvédelem
A) Az adatkezelés tárgya:	A Szolgáltatás részeként csomagszűrés, vírus- és spamvédelem és behatolásvédelem nyújtása
B) Az adatkezelés jellege és célja:	a Szolgáltatás nyújtásához szükséges gyűjtés, rögzítés, rendszerezés, tárolás, lekérdezés, betekintés, törlés és más, a Szolgáltatás szerződésszerű nyújtásához szükséges adatkezelési műveletek végzése a Szolgáltatás nyújtása és az Adatfeldolgozó szerződésszerű teljesítése céljából
C) Az adatkezelés időtartama:	IÁSZF törzsrész *A személyes adatok kezelésének időtartama* pont szerint
D) Az érintettek kategóriái:	Az Adatkezelővel szerződő vagy vele egyébként ügyfélkapcsolatban, üzleti kapcsolatban vagy más hasonló jogviszonyban álló természetes személy ügyfelek, ügyfélk, felhasználók, partnerek stb. (a továbbiakban együtt: Partnerek), továbbá az Adatkezelő, illetve Partnereinek munkavállalói vagy munkavégzésre irányuló egyéb jogviszony keretében velük kapcsolatban álló természetes személyek, esetlegesen a Partnerek ügyfelei, ügyféli, felhasználói, üzleti partnerei, illetve ezek munkavállalói vagy velük munkavégzésre irányuló egyéb jogviszonyban álló személyek (a továbbiakban együtt: Érintettek)
E) A kezelt személyes adatok kategóriái	A nyújtott szolgáltatással kapcsolatban továbbított azonosító adatok (pl. egyedi felhasználói azonosító, felhasználói név, Mac/IP cím) és webes forgalmi adatok, illetve a szolgáltatás nyújtása során keletkezett adatok
F) Az igénybe vett és az Adatkezelő által jóváhagyott al-adatfeldolgozók:	Al-adatfeldolgozó igénybevételére nem kerül sor
G) Az Adatfeldolgozó általi tevékenységhez kapcsolódó technikai és szervezési intézkedések	IÁSZF törzsrész *Az adatkezelés biztonsága* pont szerint

Ha az Adatkezelő bármikor a szolgáltatás nyújtása során azt észleli, hogy az adatfeldolgozás, illetve az érintett személyes adatok jellemzői a fent leírtaktól eltérnek, az Adatkezelő köteles kezdeményezni a fenti táblázatban leírtak aktualizálását.

12. Jogszabálytól, IÁSZF törzsszövegtől eltérő feltételek

A kapcsolattartás és az ügyfélszolgálat elérhetősége eltér az IÁSZF törzsszövegben meghatározottaktól. Ügyfél tudomásul veszi, hogy a Szolgáltató – tekintettel a szolgáltatás jellegére - a szándékosan okozott, továbbá emberi életet, testi épséget vagy egészséget megkárosító szerződésszegés kivételével kártérítési felelősségét kizárja.