10. számú melléklet: CTRL Menedzselt határvédelem

1. Szolgáltatás meghatározása

A CTRL Menedzselt határvédelem szolgáltatás keretében Szolgáltató tulajdonában álló központi, georedundáns 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 georedundáns központi rendszerrel, 99,9%-os rendelkezésre állással.

2. Szolgáltatási csomagok:

2.1 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

2.1.1 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.)

2.2 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

2.2.1 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.

2.2.2 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.

2.2.3 Alkalmazás kontroll

- Tiltásra kerülő alkalmazáskategóriák:

botnet
p2p
proxy

- Átengedésre kerülő alkalmazáskategóriák:

all other known applications
Gyártói adatbázisban még nem szereplő alkalmazás

2.3 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

2.4 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

2.5 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

3. Szolgáltatás igénybevételének feltételei

A szolgáltatás sikeres létesítéséhez és az igénybevételéhez szükséges az Előfizető által pontosan kitöltött Adatbekérő(k) átadása a Szolgáltatónak.

- **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).

- 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).
- A végponti tűzfaleszköz elhelyezése során biztosítani kell Előfizetőnek a Szolgáltató számára, hogy a tűzfaleszköz az Előfizető internet elérése és az internetelérést fogadó router közé kerülhessen.
- Fenti feltételeket Előfizető díjmentesen biztosítja a szolgáltatás nyújtásához.

- **Létesítés folyamata**: A szolgáltatás létesítettnek minősül, ha Szolgáltató Ügyfél telephelyén létesítette a Szolgáltató tulajdonában lévő tűzfaleszközt.

4. Szolgáltatás díjazása

A szolgáltatás ellenértéket az Egyedi Szolgáltatási Szerződés tartalmazza.

5. Rendelkezésre állás

Szolgáltatási szintek (SLA): A Starter, Basic, Standard és Professional csomagok SLA vállalásai különböző értékeket tartalmaznak az alábbi táblázat szerint:

Szolgáltatási szint megnevezése	**Szolgáltatási szint tartalma**	**Értéke**
A gyártó által kibocsátott frissítések, javítások telepítése	Szolgáltató a gyártó által díjmentesen kibocsátott, az Előfizető rendszere szempontjából releváns frissítéseket, biztonsági javításokat rendszeresen, a kockázatoknak és a sérülékenység súlyának megfelelő időtartamon belül telepíti. A karbantartási időszak nem számít bele a rendelkezési állás idejébe.	A frissítések átvezetéséről Ügyfelünket min. 24 órával megelőzőleg értesítjük.
Hibaelhárítás rendelkezésre állása	Szolgáltató vállalja, hogy a szolgáltatás nem megfelelő működése esetén a hibaelhárítást az adott időszakra értelmezett szolgáltatásként biztosítja.	7x24
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.	Megkezdés 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.	Starter: - Basic: - Standard: havi Professional: heti
Éves rendelkezésre állás	Naptári év: 365 nap. Szolgáltató vállalja, hogy az év 365 napjában elérhető a szolgáltatás.	99,9%

Az SLA alkalmazásának korlátai:

- Vis Major esetén;
- Szolgáltató által szükségesnek ítélt sürgősséggel elvégzendő különleges beavatkozások, melyek célja az infrastruktúra biztonságát és/vagy stabilitását és/vagy integritását érintő veszélyek elhárítása.

6. 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 Előfizető 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 Előfizetőnek 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.

7. 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

8. Hiba! A hivatkozási forrás nem található.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, előfizetők, 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, előfizetői, 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.

9. 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.