**Az Internet felőli túlterheléses (DDoS, DoS) típusú támadások elleni védelem kialakítása céleszköz bevezetésével, valamint elavult tűzfalvédelmi rendszer kiváltása új generációs, korszerű tűzfal rendszerrel – Műszaki specifikáció**

**1/a. Túlterheléses típusú támadások elleni védelem kialakítása céleszköz bevezetésével.**

2db fizikai gyártói appliance beszerzését tervezzük, mivel a hálózatunknak 2 db független Internet kijárata van. A rendelkezésre állás növelése érdekében dedikált eszközöket kérünk a védelemre, valamint külön eszközt a menedzsmentre, mely utóbbit – költségtakarékossági szempontok miatt – az 1/b. pontban meghatározott külső tűzfal szoftver menedzsment eszközével (pl.: CheckPoint Smart Event) kell kezelni.

**Elvárt funkciók:**

A megoldásnak rendelkeznie kell legalább 2Gb-es tisztítókapacitással (1 Gb full duplex-ben).

Az eszköz redundáns táppal rendelkezzen.

Network és Application flood elleni védelem is kell tudni biztosítani az alábbi rétegekben:

* network layer -volumetric attack (UDP flood, ICMP flood),
* server layer - SYN flood, Low and Slow attack,
* application layer - SSL, worms, sip, DNS, FTP, SQL,Web,Mail,
* "elárasztás" esetén UDP,TCP SYN, TCP RST, ICMP flood elleni védelem,
* Application flood esetén szignatúra alapú vizsgálat,
* folyamatosan frissülő szignatúra adatbázis,
* személyre szabott minták létrehozásának lehetősége.

A szállított rendszer On-premise megoldás legyen, viszont rendelkezzen olyan funkcionális lehetőséggel, hogy felhő alapú védelmet is tudjon kezelni ,amennyiben az eszköz tisztító-kapacitásánál túlmutat a támadás nagysága (hybrid - Scrubbing), hogy minimalizálni tudjuk a szolgáltatás kieséseket és azok idejét.

Támadás esetén azonnali beavatkozás (detektálás és blokkolás) lehetősége on-premise megoldás esetén.

SSL alapú támadás detektálása, megakadályozása

A folyamatosan áramló forgalomnál képes legyen alkalmazkodni az adott hálózati környezethez (integrálódni), megváltozott forgalmi magatartás figyelése alapján képes legyen különbséget tenni legitim és káros forgalom között (learning mode).

Képes legyen beavatkozni "Low and Slow" típusú támadások esetén.

Fejlett menedzsment képességek, melyek folyamatos monitorozási lehetőség biztosítsa DDoS támadás esetén.

Forgalmi logok nyomon követése, gyanús forgalomnál támadásoknál beavatkozáshoz szükséges ajánlás megadása.

A Felhőszolgáltatással kiegészülve a megoldás Cloud-jának képesnek kell lennie 7x24-es support biztosításra.

Az on-premise eszköznél a forgalom átvitelekor előállt késleltetés 60 micro szecundum alatt legyen.

Az alábbi tunneling protokollokat kell tudnia támogatni: GTP,GRE,L2TP,MPLS,802.1q vlan.

On-premise megoldás esetén az inline eszközök legyenek képesek HA üzemmódban működni.

Detektálás és blokkolás IPv6 esetén.

Az On-premise eszköz meghibásodás esetén legyen képes fail-open/fail-close üzemmódra kapcsolni (copper esetén maga az eszköz, fiber esetén pedig külső eszköz bevonásával).

Geo Protection képesség.

A Check Point security management rendszerünkből szabályozható, felügyelhető legyen, oda továbbítson logokat, ahol az események feldolgozása és intézkedések foganatosítása lehetséges.

**Beszerzendő eszközök mintakonfigurációja:**

* CPAP-DP2006-D-SME   
  DDoS Protector 2006 with SME Dual Power Supply AC 2 db
* CPCES-CO-STANDARD-ADD  
  Standard Collaborative Enterprise Support For 1 Year 2x 1 év

**Gyártói 1 év teljeskörű garancia, mintafrissítések biztosítása.**

**A megvalósított rendszerre a megoldás szállítójának 1 év jótállást kell vállalnia.**

**A megoldás szállítójának az alábbi feladatokat kell elvégezni az implementáció során:**

* felmérés, tervezés (fizikai, logikai)
* installáció
* integráció
* konfiguráció
* finomhangolás
* tesztelés
* üzemeltetői oktatás
* projekt menedzsment, minőségbiztosítás

**A megoldás szállítójának az alábbi dokumentációt kell tudni biztosítani az implementáció során**

* HLD és LLD szintű tervezett dokumentáció,
* Implementációs-terv dokumentáció,
* Megvalósulási dokumentáció (végleges rendszerterv),
* Üzemeltetési dokumentáció.

A feladat teljesítésének határideje: **2017. 06. 10.**

**1/b. Szoftver beszerzése elavult tűzfalvédelmi rendszer új generációs, korszerű rendszerrel való kiváltásához**

***A belső és a tűzfal tekintetében heterogén tűzfalvédelmi rendszert kívánunk kialakítani, ezért a jelen eljárásban kialakítandó új generációs külső tűzfalvédelmi megoldás nem lehet ugyanazon gyártó terméke, mint a tavaly bevezetett belső tűzfalvédelmi rendszeré, azaz nem lehet Fortinet.***

***A gyártó legyen a vezetők között a Gartner, mint független szervezet utóbbi 3 évben kiadott nagyvállalati határvédelmi rendszer megoldások kategóriájában.***

**Az új tűzfal rendszerre vonatkozó funkcionális követelmények:**

* A jelen beszerzés biztonsági szoftver licence-re vonatkozik, de a megoldás legyen később felépíthető, átmigrálható gyártói appliance eszközökre is.
* A jelen beszerzésben, implementációban az új generációs tűzfalvédelmi szoftver terméknek 3rd party szerver-en való futtatása szükséges (2 db DL 380 G9) virtualizációs platform alkalmazása nélkül. Azonban a megajánlott szoftver megoldás támogassa, illetve biztosítson lehetőséget, jogot virtuális környezetben való használatra is.
* A megoldásnak Stateful Inspection alapú részletes vizsgálatot kell végeznie a hálózati forgalomban, a kommunikációs folyamatok és alkalmazás állapotok figyelembe vételével.
* A megoldásnak biztosítania kell időszakra vonatkozó, ún. időintervallum illetve lejárati dátum alapú szabályok használatát is.
* A megoldásnak biztosítani kell aktív-passzív és aktív-aktív állapottartó klaszterműködést egyaránt, jelen kiépítésben 2 tagú klaszter a cél.
* A Microsoft Active Directory alapú felhasználói adat azonosításhoz ne legyen szükség a domain controllerekre telepítendő agent szoftverre, valamint a szoftver tudjon LDAP kompatibilis (eDirectory alapú) authentikációt is realizálni.
* Rendelkezzen belső tanúsítvány kiadóval (CA), illetve támogassa a külső CA integrálását is.
* A kapcsolódó menedzsment támogasson adminisztrátori szerepköröket, legyen például elkülöníthető a szabályrendszer módosítás és a forgalmi napló megtekintése.
* A menedzsment megoldás adjon találati, adott szabályon látható használati adatokat (pl. hit) az egyes kommunikációs szabályok esetén.
* Végezzen szabályrendszer ellenőrzést, amely azonosítja az átfedő szabályokat és figyelmeztet azokra.
* A megoldás legyen képes a napló állományok automatikus rotálására, beállított időzítés és/vagy file méret alapján.
* A megoldás minden tűzfal node esetében adjon áttekintést az alábbi paraméterekről: OS verzió, CPU és memória használat, lemezterület kihasználtsága.
* A megoldás jelen kiépítésben rendelkezzen a tradicionális tűzfal képességeken kívül fejlettebb biztonsági funkciókkal is. Ezek a további funkciókat belső komponensekkel biztosítsa külön külső eszköz használata nélkül (takarékosság, és modulok közti hatékonyabb együttműködés okán), mint:
  + URL Filtering
  + Application Control
  + DLP (csak a funkció lehetősége legyen meg, a későbbi bevezethetőség miatt)
  + IPS
  + AntiVirus (+AntiBot)
  + SSL Inspection
* Az eszköz legyen képes szofisztikált szabályrendszeri csoportok kezelésére (exclusion group – kivétel kezelés).

**Mintakonfiguráció, 1 éves kiemelt gyártói garanciával, és teljes körű határvédelmi, menedzsment és next generation védelmi frissítésekkel:**

**CPSG-8C-NGTX**

Security Gateway software for 8 cores with Next Generation Threat Prevention and SandBlast™ (NGTX) Package **1db**

**CPSG-8C-NGTX-HA**

Security Gateway software for 8 cores with Next Generation Threat Prevention and SandBlast™ (NGTX) Package – HA **1db**

**STANDARD-CES**

Collaborative Enterprise Support, 1 year **1 év**

**CPSM-NGSM5**

Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) **1 év**

**CPCES-CO-STANDARD-ADD**

Standard Collaborative Enterprise Support For 1 Year **1 év**

A szoftver leszállításának határideje: **2017. 06. 10.**

**A fenti szoftver üzembe helyezési feladatainak elvégzése**

* Migrációs feladat elvégzése,
* műszaki egyeztetés, felmérés, szabályok konszolidálása, redesign,
* Security Gateway és Management Installáció,
* Zorp policy migrálása az új tűzfalba (pl.: Check Point-ba), többi alrendszer (Cisco, Fortinet bevonásával).
* NGTP modulok beállítása,
* átállás, átállást követő napi helyszíni felügyelet,
* rendszer és megvalósulási dokumentáció (rendszerterv, rendszerbiztonsági terv, üzemeltetői dokumentáció)
* üzemeltetői oktatás,
* logisztika és külső projekt koordináció, valamint projektadminisztráció.

A feladat teljesítésének határideje: **2017. 08. 31.**

**Az 1/a. és 1/b. pontok tekintetében az ajánlott megoldás gyártójára vonatkozó követelmény:**

• A megajánlott megoldás gyártója rendelkezzen minimum 15 év tapasztalattal az Internet Biztonsági piacon.