1. számú melléklet

Műszaki leírás

DDoS eszköz korszerűsítése

A meglévő, gyártó által már nem támogatott 2 db DDOS (CPAP-DP2006-D-SME DDoS Protector 2006 with SME Dual Power Supply AC) eszközünk helyett szintén 2 db (mivel a hálózatunknak 2 db független Internet kijárata van) új, korszerűbb, fizikai gyártói appliance beszerzését tervezzük. A rendelkezésre állás szinten tartása érdekében dedikált eszközöket kérünk a védelemre.

Funkcionális követelmények (műszakilag egyenértékű termékekre vonatkozó követelmények)

A megoldásnak rendelkeznie kell legalább 2 Gbit/s tisztítókapacitással (6 Gbit/s 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 DDoS management eszköz virtuális kiépítésben valósuljon meg

A szállítandó DDoS megoldás riasztásai/logjai legyen integrálható a már meglévő Check Point Security Management-el (SmartEvent, SmartLog).

Az eszközök rendelkezzenek legalábbi 1 éves gyártói támogatással, a Standard Collaborative Enterprise Support szintnek megfelelően.

A beszerzendő eszközzel szemben támasztott technikai követelmények (műszakilag egyenértékű termékekre vonatkozó követelmények)

Legnagyobb támadási kapacitás (Gbps)	6, vagy nagyobb
Legnagyobb tisztított forgalom áteresztése (Gbps)	2, vagy nagyobb
Egyidejű támadási munkamenetek száma	korlátlan
Maximális árasztásos DDoS támadás elleni védelem (PPS)	7.2M, vagy nagyobb
SSL/TLS CPS (RSA 2K)	20K, vagy nagyobb
Késleltetés	kevesebb mint 60 micro szekundum, vagy kisebb
Hálózati működés	Transzparens L2 továbbítás/IP továbbítás
Telepítési módok	In-line; SPAN Port Monitoring; Copy Port Monitoring; local out-of-path; Out-of-path mitigation (scrubbing center solution) Sorban; SPAN port figyelés; Másolási port figyelése; helyi útvonalon kívüli; Útvonalon kívüli hatások enyhítése (scrubbing center solution)
Tunneling Protocol	VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP
IPv6	igen

Jumbo Frame	támogatott
Ellenőrző portok: 10/100/1000 Copper	6, vagy több
Ellenőrző portok: 1/10 GbE SFP+	2, vagy több
Rack hely szükséglet	1U
Energiafelhasználás	max 140W

A beszerzendő eszköz ajánlatkérő által meghatározott mintakonfigurációja

Cikkszám	Megnevezés	Mennyiség	Mennyiségi egység
CPAP-DP6-2-SME	DDoS Protector 6-2 Appliance providing 6Gbps attack mitigation and 2Gbps legitimate throughput	2	db
CPCES-CO-STANDARD-ADD	Standard Collaborative Enterprise Support 1 Year	1	db
CPAC-PSU-AC-AL5208	Single AC Power Supply- SSL Protector 5208	2	db
CPCES-CO-STANDARD-ADD	Standard Collaborative Enterprise Support 1 Year	1	db
CPSM-DP-VM-VA2-1Y	DDoS Management VA2 Virtual Appliance with Application Performance Monitoring for management of 2 DDoS Protector physical devices for 1 year	1	db

Amennyiben az ajánlatkérő a közbeszerzési dokumentumokban meghatározott gyártmányú vagy eredetű dologra hivatkozik valamely beszerzési tárgy tekintetében, azzal egyenértékű gyártmányú vagy eredetű dolgot is elfogad a közbeszerzési eljárásokban az alkalmasság és a kizáró okok igazolásának, valamint a közbeszerzési műszaki leírás meghatározásának módjáról szóló 321/2015. (X. 30.) Korm. rendelet 46. § (3) bekezdése alapján.

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, migráció
- konfiguráció
- finomhangolás
- tesztelés
- üzemeltetői oktatás

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

- Megvalósulási dokumentáció (végleges rendszerterv),
- Üzemeltetési dokumentáció frissítése.

A feladat teljesítésének határideje: **2022. június 30.**