1. sz. melléklet

V. fejezet

Elavult switchek, belső tűzfal rendszer cseréje (888/2024)

3. rész: Belső tűzfal- és behatolás megelőző rendszer cseréje

Műszaki leírás

Az Országgyűlés Hivatala 2015 óta rendelkezik Fortigate belső tűzfalvédelmi rendszerrel, amely behatolásmegelőző (IPS) funkciókat is egyaránt ellát, így a rendszer üzemeltetéséhez szükséges humánerőforrással, illetve üzemeltetői/rendszeradminsztrátori kompetenciával rendelkezünk. Azonban a rendszer fizikai appliance-einek gyártói támogatása hamarosan megszűnik, ezért ezek helyett új eszközöket szükséges beszerezni, amit a gerinchálózati eszközeink sávszélesség-növeléséhez igazítva tervez megtenni az ajánlatkérő, amely illeszkedik a folyamatosan növekvő teljesítmény igényekhez is. Ezzel szinkronban nemcsak a fizikai eszközöket kívánja ajánlatkérő cserélni, hanem az évről-évre növekvő teljesítmény szükséglet kielégítésére konfigurációs változtatást is végre kívánja hajtani, mely alapján az ajánlatkérő az aktív-passzív belső tűzfal és IPS működési módról aktív-aktívra váltana, hogy a fejlesztéssel 4-6-szoros sebesség-, illetve teljesítménynövekedést realizáljon a jelenlegi állapothoz képest.

Az új belső tűzfalvédelmi és IPS rendszernek általánosan a lenti követelményeknek kell megfelelnie:

- Megfelelően nagy teljesítmény a várható életciklus alatt.
- Széleskörű és modern hálózatbiztonsági eszköz- és funkciókészlet.
- A meglévő Cisco és Check Point rendszereinkkel való könnyű illeszthetőség.
- A piacon az elsők között rangsorolt tűzfal/security gyártó megoldása legyen.
- A meglévő belső tűzfal rendszerről az új rendszerre való migráció a meglévő hálózati és tűzfal/IPS infrastruktúra jelentős áttervezése és átépítése nélkül kell legyen megvalósítható, tekintettel a szűk leállási ablakokra, valamint a belső tűzfal és IPS infrastruktúra kritikus elemeire.

Az új belső tűzfal eszközök mellett a tűzfalhoz közvetlenül kapcsolódó loggyűjtő és analizáló rendszer cseréjét is tervezi az ajánlatkérő. Az új belső tűzfal eszközök és az új loggyűjtő rendszer elvárt paraméterei a következő szerint kerül részletezésre.

A belső tűzfal és IPS rendszer

Két db olyan nagy teljesítményű tűzfal berendezés beszerzését tervezi az ajánlatkérő, amelyek képesek az IPS-funkciókat a tűzfal funkciókkal együtt integráltan megvalósítani.

Mivel a környezet igen komplex és a rendszer újratervezése nem, vagy csak erősen korlátozott mértékben lehetséges, ezért az új eszközöknek jól kell illeszkedniük a meglévő kapcsolódó rendszerekhez.

Az új berendezéseknek teljeskörű funkcionális virtualizációra képesnek kell lennie, tehát kialakíthatóak kell legyenek rajtuk ún. virtuális tűzfalak (virt-system, context stb.), melyeknek minden olyan funkciót meg kell tudni valósítani, mint az alaprendszernek, pl. webfiltering, antivírus szűrés, IPS és a többi.

Az új eszközöknek képesnek kell lennie a virtuális tűzfal példányokat egyidőben különböző típusú üzemmódban használni, pl. 3 db Layer 3 route-olt üzemmódú és 2 Layer 2 bridge-elt üzemmódú példány egyidejű futtatása.

A biztonsági funkcióknak (IPS, webfiltering stb.) – a hálózati forgalomtovábbítási üzemmódtól függetlenül – minden példány esetében elérhetőnek és használhatónak kell lennie.

A tűzfal berendezéseknek egyenként a következőkben részletezett jellemzőkkel kell rendelkeznie:

Interface-ek és fizikai jellemzők:

- Legfeljebb 2 RU.
- Redundáns tápegységek, melyek hot-swap képesek.
- TPM (Trusted Platform Module) chip a titkosító kulcsok biztonságos tárolására.
- Legalább 4 db port QSFP28/QSFP+ 100G/40G interface modulhely.
- Legalább 16 db port SFP28/SFP+ 25G/10G interface modulhely.
- Legalább 16 db port 10G/1G RJ45 interface.
- Legalább 2 db port SFP+ 10G HA-interface modulhely.
- Legalább 2 db port 1GE RJ45 management interface.

A management interface kivételével mindegyik produktív célú interface hardveres gyorsítással is kell, hogy rendelkezzen (hardware-assisted/accelerated forwarding).

Elvárt teljesítményparaméterek:

- IPv4 firewall throughput [1500 byte UDP]: legalább 198 Gbps
- IPv4 firewall throughput [512 byte UDP]: legalább 196 Gbps
- IPv4 firewall throughput [64 byte UDP]: legalább 140 Gbps
- IPv6 firewall throughput [1500 byte UDP]: legalább 198 Gbps
- IPv6 firewall throughput [512 byte UDP]: legalább 196 Gbps
- IPv6 firewall throughput [64 byte UDP]: legalább 140 Gbps
- Firewall latency [64 byte UDP]: legfeljebb 3,5 micro secundum
- Firewall throughput [Mpps]: legalább 210 Mpps
- Egyidejű firewall-session maximum [TCP]: legalább 24 millió
- Új-tűzfal-session per másodperc [TCP]: legalább 1 millió
- Tűzfal-szabályok száma maximum: legalább 100.000
- IPSEC VPN throughput [512 byte]: legalább 55 Gbps
- SSL-VPN throughput: legalább 16 Gbps
- SSL-inspection throughput [IPS + átlagos HTTPS forgalom]: legalább 20 Gbps
- SSL-inspection connection-per-second [IPS + átlagos HTTPS forgalom]: legalább 16000
- SSL-inspection egyidejű session-ök max. [IPS plusz átlagos HTTPS forgalom]: legalább 2,7 millió
- IPS throughput [Enterprise-mix forgalom, FW + IPS + Logging]: legalább 31 Gbps
- NGFW throughput [Enterprise-mix, FW + IPS + AppControl + Logging]: legalább 27 Gbps
- Threat Protection throughput [Enterprise-mix, NGFW + IPS + AppControl + Malware Protection + Logging] legalább 25 Gbps

Tűzfal architektúra: stateful-firewall, opcionálisan proxy módú firewall kialakítási lehetőséggel.

Elvárt gateway-szintű biztonsági szűrési funkciók és egyéb képességek:

- SSL-inspection: certificate-inspection és deep-inspection (decryption/re-encryption)
- IPS Intrusion Prevention System
- Anti-virus szűrés
- Webfiltering, URL filtering
- DNS filtering
- Application Control
- File filter
- Email filter
- VoIP filter
- Dinamikus routing, IPv4 és IPv6 is: RIPv2, RIPng, OSPFv2, OSPFv3, IS-IS, BGPv4, BGPv6
- Multicast routing: IGMPv2, IGMPv3, PIM-SM, PIM-SSM
- Network Address Translation: NAT44, NAT66, NAT46, NAT64
- SSLVPN
- IPSEC VPN (IKEv2)
- Virtuális tűzfalak száma: alapértelmezetten legalább 10 db, de licenccel tovább bővíthető legyen.
- High-Availability kialakítási lehetőségek: Active-Active, Active-Standby, Clustering.
- Logging: UDP és TCP alapú Syslog, teljes session naplózása (start-stop), biztonsági esemény esetén történő naplózás
- Automatizációs képességek: teljes értékű REST API megléte
- Integrált One-Time-Password szerver funkció:

  a berendezés rendelkezzen a tűzfal operációs rendszeren belül elérhető OTP szerver funkcióval, mely a tűzfalon kívüli plusz eszköz vagy erőforrás igénybevétele nélkül lehetővé teszi token-alapú erős authentikáció használatát akár tűzfal-adminisztráció akár felhasználói vagy tűzfal-adminisztrátori VPN kapcsolatok kialakítása esetén.

Gyártói biztonsági információkra vonatkozó előfizetés

Az ajánlatkérő célja, hogy közel minden a gyártó által biztosított előfizetés alapú, folyamatosan frissülő biztonsági-információ (security intelligence) rendelkezésére álljon, tehát olyan előfizetési szolgáltatást szeretne, amely által a tűzfal a legfrissebb biztonsági információkkal rendelkezhet majd (automatikus letöltések révén) a következőkre:

- IPS szignatúra adatbázis
- Mesterséges Intelligencia alapú malware-védelem (AI-based Inline Malware Protection)
- Inline CASB
- DLP (Data Loss Prevention)
- Application Control
- Advanced Malware Protecton
- URL-filtering
- DNS-filtering
- Video-filtering
- Anti-Spam
- Attack Surface Security

Transceiver modulok:

A belső tűzfal eszközök az alábbi SFP+ SFP28 és QSFP+ modulokkal legyenek feltöltve:

- 10GE SFP+ transceiver module, 10km long-range 4 db (tűzfalanként 2 db)
- 40GE QSFP+ transceiver module, short-range 8 db (tűzfalanként 4 db)
- 10GE SFP+ transceiver module, short-range 16 db (tűzfalanként 8 db)
- 25GE/10GE Dual Rate SFP28 transceiver, short-range 16 db (tűzfalanként 8 db)

Belső tűzfal és IPS eszközök loggyűjtő eszközének cseréje

A belső tűzfal eszközökhöz teljes mértékben illeszkedő és integrálható loggyűjtő és analizáló megoldást szeretne az ajánlatkérő, mely a következő jellemzőkkel rendelkezik:

- A belső tűzfalakhoz IPSEC tunnelen képes csatlakozni
- Biztonságos IPSEC csatornán képes fogadni a TCP vagy UDP alapú Syslog üzeneteket
- Virtuális kivitel: 1 db virtual-appliance, mely VMware ESXi környezetbe kell illeszkedjen.
- Teljesítménye: 2x5 GB/log/nap licenc (összesen 10 GB/log/nap kapacitás szükséges).
- A rendszernek képesnek kell lennie ún. playbook-ok futtatására melyek indítási feltételeként– a logokra vonatkozó – összetett feltételrendszert lehetséges meghatározni.
- A rendszernek képesnek kell lennie testreszabható ad-hoc és ütemezett riportok generálására és azok email-ben való kiküldésére.
- Addicionális előfizetéses szolgáltatásokkal rendelkezzen:
    - IOC Indicators-of-Compromise
    - Security Automation Service
    - Outbreak Detection Service

Gyártói támogatás

A tűzfal eszközökre és a transceiver-ekre a gyártói terméktámogatást (jótállást) 5 (60 hónap) évre kéri az ajánlatkérő és a fent említett biztonsági információkra vonatkozó előfizetési szolgáltatást szintén 5 (60 hónap) évre. A gyártói support típusának olyan szintűnek kell lennie, hogy fizikai appliance eszközhiba esetén legkésőbb a következő munkanapra csereeszközt kell, hogy biztosítson.

Az új belső tűzfal logging és analitikai eszközre szintén 5 év gyártói támogatást és 5 év előfizetést kér az ajánlatkérő a fent részletezett szolgáltatásokra vonatkozóan.

Valamennyi gyártói jótállásnak és elfizetésnek ugyanarra a kezdő és lejárati dátumra kell esnie.

Mintakonfiguráció:

A lenti mintakonfigurációk a fentiekben meghatározott műszaki követelményeknek maradéktalanul eleget tesznek, de Ajánlatkérő a lenti mintakonfigurációban megnevezett termékekkel műszakilag egyenértékű termékek megajánlását is elfogadja.

Sorszám	Cikkszám	Megnevezés	Menny.
1	FG-2600F	FortiGate-2600F 4 x 100GE/40GE QSFP28 slots, 16 x 25GE/10GE SFP28 slots, 16 x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies	2
2	FC-10-F26HF-809-02-60	FortiGate-2600F 5 Year Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)	2
3	FN-TRAN-SFP+LR	10GE SFP+ transceiver module, long range 10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots	4
4	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range 40GE QSFP+ transceiver module, short range for systems with QSFP+ Slots	8
5	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	16
6	FN-TRAN-SFP28-SR	25GE SFP28 transceiver module, short range 25GE/10GE Dual Rate SFP28 transceiver module, short range for systems with SFP28/SFP+ slots	16
7	FC1-10-AZVMS-465-01-60	FortiAnalyzer-VM Subscription License with Support 5 Year Subscription license for 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service.	2