Príloha č. 1 - Opis predmetu zákazky

1. PREDMET VEREJNÉHO OBSTARÁVANIA

Predmetom zákazky je dodanie informačno-komunikačných technológií proxy riešenia vrátane potrebného výpočtového hardvéru a súvisiacich služieb a najmä služby súvisiacej s poskytovaním záručného servisu a dopravy na miesto dodania.
Podrobná minimálna technická špecifikácia proxy riešenia je uvedená v nasledujúcich bodoch 3 až 14.

2. ŠPECIFIKÁCIA PREDMETU ZÁKAZKY

V rámci zvyšovania úrovne kybernetickej bezpečnosti, dostupnosti a kvality prevádzkovaných aplikácií a v súvislosti s proaktívnou stratégiou prístupu z pohľadu kybernetickej bezpečnosti verejný obstarávateľ požaduje dodanie a nasadenie proxy serverov, ktoré zvyšujú bezpečnosť tým, že fungujú ako bariéra medzi používateľmi a internetom. Zároveň pomáhajú chrániť pred škodlivými stránkami a útokmi filtrovaním škodlivého obsahu.

Verejný obstarávateľ požaduje, aby dodané riešenie spĺňalo parametre a funkcionality, ktoré sú definované prostredníctvom funkčných a nefunkčných požiadaviek spolu uvedených v bodoch 3 až 14 časti Opis predmetu zákazky. Verejný obstarávateľ požaduje jednotné riešenie zabezpečujúce plnú funkčnú kompatibilitu a centralizovanú správu bez potreby dodatočného softvéru na cieľových zariadeniach.

3. ROZSAH ZÁKAZKY A LICENČNÉ PODMIENKY

Riešenie musí byť dodané v rámci vysokej dostupnosti, tak aby výpadok jedného komponentu nespôsobil výpadok proxy služby. Čiže v rámci riešenia je požadované dodanie 2 kusov hardvérových proxy zariadení (2 kusy appliance), aby v prípade výpadku jedného zariadenia prebralo plnohodnotne funkcionalitu druhé zariadenie.

4. ZÁKLADNÉ FUNKČNÉ POŽIADAVKY:

- explicitné proxy pre web protokoly HTTP/HTTPS s podporou cache,
- implicitné nastavenie proxy (v rámci 1 boxu),
- TCP Relaying (metóda CONNECT over HTTP),
- podpora cache-ovania odpovedí (proxy cache),
- nastavenie výnimiek z cache-ovania na základe cieľovej URL/URI, web kategórie,
- manuálna úprava kategórií na základe URL , IP. Možnosť vytvárania vlastných kategórií,
- možnosť zadania požiadavky na re kategorizáciu URL alebo IP v databáze dodávateľa,
- antivírová (AV) kontrola priamo na proxy appliance. Možnosť dodatočného použitia externých AV pomocou ICAP (Internet Content Adaptation Protocol – protokol na filtrovanie a úpravu internetového obsahu),
- dešifrovanie a inšpekcia SSL/TLS komunikácie,
- nastavenie výnimiek z SSL/TLS inšpekcie resp. vynútenie inšpekcie SSL/TLS, komunikácie na základe URL, kategórie URL, používateľa, zdrojovej IP adresy klienta alebo certifikátu servera,
- kontrola typu sťahovaných objektov/súborov na základe skutočného obsahu (nesmie byť detegovaný iba pomocou prípony alebo iba pomocou MIME type),
- možnosť blokovania určitých typov objektov/súborov (spustiteľné súbory, ActiveX, Java Script, Flash video, heslované/šifrované súbory a súborové archívy apod.) a možnosť nastavenia výnimiek z blokovania takýchto objektov,

- podpora kontroly prístupu k web aplikáciám (WEB 2.0 - typicky Facebook, Twitter, cloud storage a pod. až na úroveň jednotlivých používateľských úkonov - napr. zakázať publikovanie príspevkov, upload/download príloh atď.),
- detekcia a blokovanie komunikácie z/na známe zdroje malware, spyware a Botnety,
- detekcia a možnosť blokovania klientskej komunikácie na iné proxy servery, web-anonymizéry. Pokiaľ sa používa detekcia aj formou databázy, potom musí výrobca zabezpečiť pravidelnú aktualizáciu týchto zdrojov,
- podpora reputačného hodnotenia cieľových serverov (dodatok ku statickej kategorizácii URL/IP). Výrobca zabezpečuje pravidelnú aktualizáciu týchto zdrojov,
- pokročilá analýza hrozieb na základe definícií dodávaných a updatovaných výrobcom,
- možnosť manipulácie s HTTP hlavičkou (min. X-Forwarded-For a Via),
- FTP proxy,
- Kategorizácia neznámych/nezaradených URL/IP adries,
- Podpora enginu pre realtime analýzu obrázkov. Systém musí byť schopný detegovať zobrazovanie drog, alkoholu, zbraní, pornografie, extrémizmu, gamblingu a iného nevhodného obsahu,
- Obmedzenie šírky pásma pre streamované dáta (video, audio).

5. VÝKONNOSTNÉ PARAMETRE / REDUNDANCIA:

- riešenie musí poskytovať plnú redundanciu,
- riešenie musí byť schopné rozkladať komunikáciu (balancing),
- celková priepustnosť riešenia (so zapnutými funkciami AV + aplikačná kontrola + webfiltering + SSL inšpekcia (1 TCP session obsahujúca 10 HTTP requestov)) minimálne **8.000** Mbps pre každé zariadenie,
- riešenie musí byť schopné spracovať minimálne **10.000** transakcií za sekundu (so zapnutými funkciami AV + aplikačná kontrola + webfiltering + SSL inšpekcia (1 TCP session obsahujúca 10 HTTP requestov)) pre každú lokalitu/node,
- počet používateľov je **2500** (tento počet musí riešenie podporovať aj v prípade straty redundancie / výpadku jedného zariadenia),
- pripojenie do siete (per zariadenie) - min. **2x10G SFP+** vrátane SFP+
- podpora ethernet redundancie: active / standby alebo active/active LACP.

6. POŽIADAVKY NA ANTIVÍRUS:

- systém musí podporovať konfiguráciu výnimiek AV kontroly na základe URL, URI, kategórie, typu sťahovaných súborov,
- podpora kontroly archívov,
- možnosť nastavenia blokovania zaheslovaných/šifrovaných súborov/archívov,
- kontrola na základe signatúr. Výrobca zaisťuje pravidelnú aktualizáciu signatúr a prípadne ďalších definícií pre AV engine.

7. AUTENTIZÁCIA:

- autentizácia klientov voči MS Active directory,
- autentizácia klientov voči LDAP serveru (podpora LDAP aj LDAPS),
- podpora NTLM v2,
- podpora Kerberos,
- pravidlá pre výnimky z autentizácie na základe klientskej IP adresy / siete a cieľovej URL,
- autentizácia klientov voči lokálnej databáze.

8. AUTORIZÁCIA:

- povoliť/zakázať požiadavky na základe IP adresy / siete klientov,
- povoliť/zakázať požiadavky na základe cieľovej URL/URI alebo ich častí,
- povoliť/zakázať požiadavky na základe kategorizácie URL,
- povoliť/zakázať požiadavky na základe hodnotenia reputácie cieľového serveru,
- povoliť/zakázať požiadavky na základe adresy Layer 4 protokolu (napr. metóda CONNECT over HTTP),
- povoliť/zakázať požiadavky na základe autentizácie používateľa alebo jeho členstva v skupine v MS AD,

- povoliť/zakázať požiadavky na základe časových údajov (čas, dátum, časové rozmedzie),
- povoliť/zakázať požiadavky s metódou POST/PUT,
- ľubovoľná kombinácia vyššie uvedených,
- prispôsobenie oznámenia pre používateľa (Block / Error / Warning / ďalšie informácie stránky).

9. MANAGEMENT:

- konfigurácia každej proxy tvoriacej HA riešenie musí byť vždy synchronizovaná s poslednou verziou zmien,
- autentizácia a autorizácia správcov systému pomocou LDAP, AD alebo RADIUS,
- podpora multi factor authentication pre správcov systému,
- min. 2 role pre správcov systému, (read-write, read-only),
- možnosť definovať používateľské role pre správcov systému (RBAC),
- aplikovanie konfiguračných zmien bez výpadku služby,
- protokol SNMP minimálne vo verzii v2c.

10. LOGOVANIE A REPORTOVANIE:

- možnosť zapnutia debugovacieho režimu pre používateľské požiadavky,
- access log (user and associated requests) - vzdialené logovanie - Syslog UDP, TCP,
- podpora tcpdump nástroja priamo na proxy s možnosťou definície filtrov,
- možnosť zasielania informácií o stave systému a jeho zmene do syslogu a pomocou SMTP,
- report využívania služieb proxy minimálne na základe zdroja (IP adresa, používateľské meno), cieľa (URL, kategórie URL) a statusu požiadavky (povolené, blokované, blokované na základe čoho), veľkosti požiadaviek/odpovedí a ďalších voliteľných parametrov,
- podpora auditného logovania prístupu správcov vrátane vykonaných zmien v konfigurácii,
- uchovávanie logov pre možnosť auditu a tvorby reportov po dobu min 3 mesiacov,
- automatické a manuálne generovanie reportov s možnosťou nastavenia automatického opakovania a odosielania pomocou SMTP.

11. INŠTALÁCIA:

- analýza a dizajn
- nasadenie a testovanie
- zarackovanie, nakáblovanie a oživenie zariadení
- update OS zariadení
- pripojenie do manažmentu a konfigurácia podľa požiadavky objenávateľa

12. ZAŠKOLENIE:

- zaškolenie 3 administrátorov v rozsahu 2 MD na implementovaných zariadeniach

13. PODPORA VÝROBCU

- Musí poskytovať podporu výrobcu 24x7 na obdobie 24 mesiacov od dodania riešenia
- Odstránenie kritickej závady do nasledujúceho pracovného dňa od identifikácie príčiny závady. Kritická závada sa rozumie závada keď nastane situácia, ktorá má závažný dopad na prevádzku alebo bezpečnosť riešenia spočívajúca napríklad v úplnom výpadku služby, existencie odhalenej bezpečnostnej zraniteľnosti, v zlyhaní režimu vysokej dostupnosti.

14. PODPORA PARTNERA

- Musí poskytovať podporu partnera 8x5 v rozsahu 20MD na zazmluvné obdobie, ktoré bude objenávateľ čerpať na vyžiadanie