Príloha č. 1

Opis predmetu zákazky - Web proxy HW zariadenie

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 rekategorizáciu URL alebo IP v databáze dodávateľa
- AV kontrola priamo na proxy appliance. Možnosť dodatočného použitia externých AV pomocou ICAP
- Dešifrovanie a inšpekcia SSL/TLS komunikácie
- Nastavenie výnimiek z SSL/TLS inšpekcie resp. vynútenie inšpekcie SSL/TLS komunikácie na základe URL, kategórie URL, užívateľa, zdrojovej IP adresy klienta alebo certifikátu servera

- Kontrola typu sťahovaných objektov/súborov na základe skutočného obsahu (nesmie byť detekovaný 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 apod. až na úroveň jednotlivých užívateľských úkonov - napr. zakázať publikovanie príspevkov, upload/download príloh atd.), prosím uveďte počet a názov podporovaných aplikácii (môže byť aj formou odkazu na web kde sú tieto informácie verejne dostupné)
- Výrobca musí garantovať podporu riešenia a všetkých jeho komponentov minimálne po dobu nasledujúcich 5 rokov
- Detekcia a blokovanie komunikácie z/na známe zdroje malware, spyware a Botnety. Výrobca musí zabezpečiť pravidelnú aktualizáciu týchto zdrojov.
- 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)
- Podpora IPv6
- FTP proxy
- Kategorizácia neznámych/nezaradených URL/IP adries
- podpora sandboxingu (vo forme HW/VM appliance a cloud riešenia)
- podpora IPS založeného na definíciách (signature-based) a technikách nevyžadujúcich definície (signature-less) schopnými zablokovať napr. domain generation algoritmus útoky, java a flash exploity a pod. Minimálne 11000 definícií dodávaných a updatovaných výrobcom
- podpora filtrovania Youtube videí pomocou kategorizácie (min. 10 kategórií dostupných out-of-box).
- podpora AI based engine pre realtime analýzu obrázkov. Systém musí byť schopný detegovať zobrazovanie drog, alkoholu, zbraní, pornografie, extrémizmu, gamblingu a iného nevhodného (Not Safe for Work) obsahu.

- podpora správy prístupu k Internetu pre mobilných klientov (PC, MAC, Linux, iOS, Android)
- Obmedzenie šírky pásma pre streamované dáta (typicky video, audio)
- Možnosť integrácie so systémom DLP napr. pomocou ICAP alebo podpora DLP priamo v proxy appliance minimálne na úrovni vyhľadávania reťazcov pomocou regexp, watermarking, fingerprinting.

Výkonnostné parametre / redundancia

- Riešenie musí poskytovať plnú redundanciu cez 2 geograficky oddelené lokality
- Riešenie musí byť schopné rozkladať komunikáciu na 2 geograficky oddelené lokality (balancing)

- Celková priepustnosť riešenia (so zapnutými funkciami AV + Aplikačná kontrola + Webfiltering + SSL inšpekcia (1 TCP session obsahujúca 10 HTTP requestov)) minimálne 5 Gbps pre každú lokalitu/node. Uveďte priepustnosť navrhovaného riešenia pri HTTP a HTTPS komunikácii (response 44k, resp uveďte detaily testu).
- Riešenie musí byť schopné obslúžiť minimálne 800 000 konkurentných TCP spojení pre každú lokalitu/node (so zapnutými funkciami AV + Aplikačná kontrola + Webfiltering + SSL inšpekcia (1 TCP session obsahujúca 10 HTTP requestov))
- 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 (uveďte hodnotu CPS, Requests Per Second , Transactions Per Second - podľa názvoslovia výrobcu).
- Počet užívateľov je 1000 (tento počet musí riešenie podporovať aj v prípade straty redundancie / výpadku jednej lokality). Riešenie musí podporovať rozšírenie počtu užívateľov pomocou licencie až na 5 násobok.
- Pripojenie do siete (per node) - min. 2xSFP+, 2x1GE RJ45/SFP porty pre data plane a 1x1GE RJ45 mgmt port
- Možnosť spoločného aj oddelených sieťových rozhraní pre in a out komunikáciu (režim one-arm / two-arm)
- Veľkosť RAM: minimálne 64GB
- Kapacita diskového priestoru: 4x 2TB HDD
- Monitoring dostupnosti a failover proxy služieb, ktoré sú nutné pre prevádzku systému (DNS servery, AD servery, NTP servery, AV, príp. ďalšie súčasti dodaného riešenia)
- Každý proxy node musí mať minimálne 1 zdroj s možnosťou doplnenia druhého zdroja napájania

- Podpora ethernet redundancie: active / standby alebo active/active LACP. Uveďte prosím spôsob redundancie.

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
- proxy musí byť schopné získavať signatúry pokrývajúce novo odhalený malware zo sandboxu ktorý používa
- kontrola na základe signatúr. Výrobca zaisťuje pravidelnú aktualizáciu signatúr a prípadne ďalších definícií pre AV engine (minimálne jeden krát v priebehu 24 hodín).

Autentizácia

- Autentizácia klientov voči MS Active directory
- Autentizácia klientov voči LDAP serveru (podpora LDAP aj LDAPS)

- Podpora NTLM v2
- Podpora NTLM v1
- Podpora Basic Auth
- Podpora Kerberos
- Pravidlá pre výnimky z autentizácie na základe klientskej IP adresy / siete a cieľovej URL
- Kontrola nastavenia parametrov cachovania autentizačných požiadaviek/odpovedí
- Možnost autentizace vůči více doménám MS AD (připojte poznámku, pokud lze pouze za použití externího agenta)
- Autentizácia klientov voči lokálnej databáze

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 užívateľa alebo jeho členstva v skupine v MS AD
- povoliť/zakázať požiadavky na základe časových údajov (čas, dátum, časové rozmedzie)
- povoli/zakázať požiadavky s metodou POST/PUT
- ľubovolná kombinácia vyššie uvedených
- Prispôsobenie oznámenia pre užívateľa (Block / Error / Warning / dalšie info stránky)

Management

- Spoločná správa všetkých proxy (v rámci redundantnej skupiny) z jedného miesta - pomocou GUI

- Konfigurácia každej proxy tvoriacej HA riešenie musí byť vždy synchronizovaná s poslednou verziou zmien
- Autentizácia a autorizácia správcov systému pomocí LDAP, AD alebo RADIUS
- Podpora multi factor authentication pre správcov systému

- Min. 2 role pre správcov systému, (read-write, read-only)

- Možnost definovat uživatelské role pro správce systému
- Aplikovanie konfiguračných zmien bez výpadku služby
- Upgrade firmware HA clustra bez výpadku služby
- SNMP v2c a v3
- Možnosť zapnutia debug režimu pre uživateľské požiadavky
- Access log (user and associated requests) - vzdialené logovanie - Syslog UDP, TCP
- Podpora tcpdump-like 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 na základe zdroja (IP adresa, užívateľské 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

Licenčné a záručné požiadavky

- Záruka a všetky potrebné licencie min. 3 roky od dátumu akceptácie. Podpora výrobcu v režime 24x7. Vlastníctvo Supportného kontraktu a licencií priamo objednávateľom. Prístup na supportný portál vo vlastníctve objednávateľa, otváranie, správa supportných ticketov priamo objednávateľom.