**Opis przedmiotu zamówienia**

Postępowanie o udzielenie zamówienia publicznego prowadzone w trybie przetargu nieograniczonego na **przedłużenie subskrypcji oraz rozbudowę systemu PROXY BlueCoat SWG (Cloud Secure Web Gateway) oraz CAS (Content Analysis and Cloud Sandboxing)**, nr PN-11/2022

| Lp. | Opis | Nr katalogowy | Ilość |
|---|---|---|---|
| **1** | Web Protection Suite 1YR<br>Zawiera:<br>1) On-premises Secure WebGateway (SWG)Cloud Secure Web Gateway(delivered as a Service);<br>2) Content Analysis and Cloud Sandboxing (CAS)Management Center and ReporterCloud SWG;<br>3) Reporting High Risk Isolation Intelligence Services(Advanced) Web Application Firewall. | WEB-PROTECT-SUB lub równoważny* | 1 600 szt. |
| **2** | Prace wdrożeniowe:<br>1) Skonfigurowanie dostarczonych subskrypcji Systemu Proxy;<br>2) Wdrożenie oraz skonfigurowanie CAS<br>3) Przygotowanie dokumentacji powykonawczej Systemu Proxy;<br>4) Zapewnienie przeglądów kwartalnych. | | |
| **3** | Dodatkowe wsparcie techniczne Wykonawcy w wymiarze 64 roboczogodzin | | |

***- opis produktu równoważnego**

System musi zostać dostarczony w postaci dedykowanych, prekonfigurowanych maszyn wirtualnych pod środowisko VMWare ESX.
System forward proxy musi składać się z następujących modułów:

a. realizującego funkcję proxy
b. moduł raportujący
c. system centralnego zarządzania
d. moduł skanujący pliki

1. Rozwiązanie systemowe musi realizować funkcję forward proxy w trybie explicit i transparent, w szczególności explicit i transparent na jednym urządzeniu.
2. System musi mieć możliwość pracy również w trybie reverse proxy na tym samym urządzeniu.
3. W obu trybach tj. forward i reverse proxy system musi realizować funkcję cachowania ruchu, w tym również video.
4. Musi być możliwe kontrolowanie cache'a poprzez politykę – np. wyłączenie cachowania dla wybranej strony czy kategorii URL.
5. Urządzenie musi obsługiwać w trybie proxy następujące protokoły: HTTP, HTTPS, FTP, FTPS, DNS. Dla pozostałych protokołów powinna być możliwość tunelowania ruchu.
6. System musi być wyposażony w dedykowane proxy dla protokołów strumieniowych – minium RTSP, RTMP, MMS, HLS, HDS i Silverlight.
7. W trybie proxy DNS system musi wpierać co najmniej:
    a. DNS sinkholing na bazie kategorii URL, w tym własne kategorie np. blacklista
    b. DNS sinkholing na bazie reputacji URL,
    c. DNS sinkholing na bazie geolokalizacji,

    d. DNS sinkholing na bazie adresu źródłowego,
    e. DNS sinkholing na bazie typu zapytania – CNAME, AXFR, MX, SOA itd.
    f. Możliwość konkatencji powyższych warunków – np. sinkholling zapytań o rekordy MX dla stron hostowanych w Chinach.
8. Dla protokołów strumieniowych system musi wspierać funkcjonalność typu split streaming – tzn. dla treści oglądanych przez wielu użytkowników strumień video ściągany z Internetu powinien być jeden, żeby nie obciążać łącza internetowego wielokrotnością przepustowości strumienia.
9. System powinien umożliwiać definicję wielu serwisów nasłuchujących dla trybu explicit proxy dla różnych sieci np. 8080 dla pracowników i 3128 dla serwerów.
10. Powinno być możliwe przypisanie polityki w zależności od portu TCP na który trafił użytkownik tj. inna polityka dla pracowników i inna dla serwerów jak wyżej.
11. Kategoryzacja adresów URL musi być oparta zarówno o statyczna, aktualizowaną przynajmniej 2 razy dziennie bazę bezpośrednio na urządzeniu jak i rozproszony serwis w chmurze analizujący w czasie rzeczywistym nieznane adresy URL (analiza dynamiczna).
12. Mechanizm dynamicznej klasyfikacji musi wspierać analizę języka polskiego.
13. System musi dokonywać kategoryzacji adresów URL w oparciu o bazę tego samego producenta.
14. System musi wspierać kategoryzację z serwisu Youtube poprzez klucz API – minimum na bazie kategorii np. Music, Film & Animation itp.
15. System musi posiadać co najmniej 80 dostępnych kategorii URL, przy czym dany URL może należeć do więcej niż jednej kategorii.
16. System musi posiadać możliwość stworzenia własnej bazy kategorii minimum whitelist i blacklist, które mogą być utrzymywane poza systemem proxy np. przez helpdesk w postaci pliku tekstowego na współdzielonym zasobie plikowym, a następnie w cykliczny sposób importowane do polityki na urządzeniu.
17. Powinna istnieć kategoria „Uncategorized", która może być akcją w polityce na wypadek, gdyby mechanizm dynamicznej klasyfikacji nie był w stanie przypisać stronie żadnej kategorii.
18. Niezależnie od mechanizmu klasyfikacji w oparciu o kategorię strony powinien istnieć mechanizm oceny reputacji danej strony uwzględniający przynajmniej 5 stopni ryzyka.
19. Możliwość konstrukcji polityki w oparciu o reputację danej strony w połączeniu z bazą kategorii np. blokuj reklamy ze stron o wysokim poziomie ryzyka.
20. Każde zapytanie o reputację strony powinno zwracać wynik w założonej przez producenta skali. Innymi słowy niedopuszczalna jest sytuacja, że mechanizm reputacji nie dostarcza żadnej informacji o ryzyku dla danej strony.
21. System musi pozwalać na blokowanie TORa, nawet w przypadku wykorzystania pluggable transport protocol.
22. System musi posiadać narzędzie graficzne do tworzenia polityk oraz mieć wbudowany język programowania dla zaawansowanych polityk.
23. Zarządzanie systemem powinno być możliwe zarówno przez interfejs graficzny (lokalna lub centralna konsola) jak i poprzez command-line. Nie powinno być ograniczeń w interfejsie command-line w stosunku do interfejsu graficznego.
24. System musi pozwalać na automatyzację zadań poprzez command-line – np. dodanie URLa do blacklisty.
25. System musi mieć możliwość tworzenia polityk w oparciu o geolokalizację – np. blokuj ruch do Chin.
26. System powinien posiadać możliwość blokowania określonych typów plików na bazie ich zawartości np. plików wykonywalnych, plików PDF, obrazków itp.

27. System musi uwierzytelniać użytkowników w oparciu o źródła takie jak: lokalna baza, NTLM lub Kerberos (w trybie bezpośrednim i z wykorzystaniem dedykowanego agenta), LDAP (Active Directory, eDirectory,), RADIUS i certyfikat.
28. System musi dawać możliwość kontroli popularnych webaplikacji z akcjami typu upload, download, post czy send. Minimalny zestaw webaplikacji: facebook, twitter, linkedin, youtube, vimeo, snapchat, google plus, gmail, google talk, google docs, sharepoint, evernote, dropbox, box, sugarsync, flickr, instagram, webex.
29. System musi dawać możliwość deszyfrowania ruchu SSL/TLS na urządzeniu w oparciu o algorytmy RSA, DH i ECDHE, zarówno w trybie forwarding proxy jak i reverse proxy.
30. Zaoferowane rozwiązanie powinno mieć możliwość rozszerzenia funkcjonalności systemu o możliwość skopiowania odszyfrowanego ruchu SSL/TLS na zewnątrz dla dowolnego protokołu opakowanego SSL/TLS.
31. System musi mieć możliwość selektywnego włączenia funkcji deszyfracji z pominięciem pewnych kategorii jak zdrowie czy usługi finansowe.
32. System musi mieć możliwość robienia wyjątków deszyfracji SSL/TLS w oparciu o adres źródłowy / podsieć.
33. W trybie rozszywania ruchu SSL system powinien dawać możliwość kontroli certyfikatu serwera, do którego łączy się użytkownik tj. minimum sprawdzenia daty ważności i łańcucha certyfikacji.
34. System musi dawać możliwość blokowania stron szyfrowanych nawet jeśli mechanizm rozszywania SSL'a jest wyłączony np. blokowanie facebooka.
35. Wykrywanie i blokowanie tunelowania w protokołach HTTP/HTTPS np. blokowanie sesji SSH na porcie 443.
36. System proxy musi wspierać filtrowanie w oparciu o wyrażenia regularne co najmniej dla następujących parametrów:
    a. HTTP URI (pełna ścieżka włącznie z query)
    b. HTTP Request Header (wszystkie nagłówki nie tylko X-***)
    c. HTTP Response Header (standardowe nagłówki i własne)
    d. HTTP Response Data
    e. Certyfikat serwera (co najmniej hostname i subject)
    f. Atrybut SAML (dowolny atrybut)
37. System musi mieć możliwość zarządzania podziałem pasma dla uprzywilejowanych usług, wsparcie QoS/ToS.
38. Blokowanie dostępu na bazie wybranych wyszukiwanych fraz np. „porno" czy „narkotyki" – tj. próba wejścia na taką stronę poprzez wyszukiwarkę powinna zostać zablokowana.
39. Moduł musi umożliwiać zablokowanie dostępu do hostów numerycznych np. https://1.2.3.4.
40. Rozwiązanie musi współpracować z zewnętrznymi skanerami antywirusowymi/antimalware za pomocą otwartego protokołu ICAP w tym jego szyfrowanej implementacji ICAPS.
41. System powinien wspierać zarówno ICAP(S) request mode jak i ICAP(S) response mode.
42. Wsparcie proxy chaining w następującym zakresie:
    a. wysyłanie ruchu do upstream proxy na bazie URI (całego URI, nie tylko domena),
    b. wysyłanie ruchu do upstream proxy na bazie podsieci adresu źródłowego IP,
    c. wysyłanie ruchu do upstream proxy na bazie podsieci adresu docelowego IP,
    d. wysyłanie ruchu do upstream proxy na bazie kategorii URL,
    e. wysyłanie ruchu do upstream proxy na bazie reputacji URL,
    f. wysyłanie ruchu do upstream proxy na bazie geolokalizacji URL,
    g. loadbalancing upstream proxy.
43. Wsparcie protokołu WCCP w wersji drugiej, możliwość działania w oparciu o ruch przekierowanych via Policy Based Routing.

44. Możliwość trzymania pliku konfiguracyjnego Proxy-Auto-Config (tzw. PAC) bezpośrednio w systemie.
45. Wsparcie wielu plików PAC w zależności od podsieci, w której znajduje się użytkownik.
46. Wsparcie mechanizmów wydajnościowych jak pipelining i websockets.
47. Wsparcie opcji Safe Search w wyszukiwarkach internetowych – co najmniej Google, Youtube, Bing, DuckDuckGo.
48. Wsparcie IPv6 zarówno w zakresie analizy ruchu jak i systemu zarządzania.
49. System musi logować co najmniej następujące informacje:
    a. Data transakcji wg lokalnego czasu,
    b. IP adres źródłowy,
    c. Login użytkownika, jeśli nastąpiło uwierzytelnienie,
    d. Kategoria URL,
    e. IP adres docelowy,
    f. Pełen URL (cała ścieżka),
    g. Referer,
    h. Hostname/subject z certyfikatu,
50. Na poziomie sieciowym system musi obsługiwać następujące funkcjonalności:
    a. VLAN
    b. LACP,
    c. statyczny routing,
    d. dynamiczny routing – co najmniej RIP,
    e. routing domains / VRF.
51. Minimalne wymagania na hardware proxy:
    a. Dwa urządzenia obsługujące pasmo co najmniej **400 Mbps** każde, przy założeniu 75% udziału SSL/TLS w ruchu i zaawansowanych politykach.
    b. Co najmniej dwa urządzenia muszą zapewnić ciągłą pracę dla 1600 użytkowników
    c. Każde urządzenie musi obsługiwać co najmniej 50 tysięcy równoległych sesji.
    d. Każde urządzenie musi posiadać minimum 8 rdzeni CPU
    e. Każde urządzenie musi być wyposażone w minimum 32 GB pamięci RAM.
    f. Każde urządzenie musi posiadać pamięć masową o całkowitej pojemności 4 x 100 GB.
52. Zaproponowane rozwiązanie systemowe musi posiadać **moduł skanowania plików** w celu wykrycia złośliwego kodu (malware).
53. Analiza antimalware przy pomocy następujących mechanizmów:
    a) Sprawdzenie reputacji plików w bazie hashy utrzymywanej przez producenta zważającej stopniowane wartości o różnych stopniach zaufania – np. „10” plik zaufany, „1” malware,
    b) Analizowanie przez jeden silnik antywirusowy AV z możliwością uruchomienia dodatkowych silników AV tak aby działały jednocześnie. Oferowane rozwiązanie musi umożliwiać uruchomienie co najmniej 2 różnych silników AV.
    c) Analiza statyczna kodu zawartego w plikach
    d) Analiza dynamiczna aka sandboxing w chmurze dostawcy rozwiązania.
    e) Własna baza hashy działająca na zasadzie białej / czarnej listy.
54. System musi umożliwiać skanować pod kątem malware wszystkie pliki bez wyjątków.
    a) System powinien umożliwiać analizę dynamiczną plików w następujących formatach: 7z-compressed, ace-compressed, arj, bzip2, ms-cab-compressed, gzip, lha, rar-compressed, tar, ms-tnef, zip, dosexec, dosexec-dll, java-archive, pdf, msword, ms-excel, ms-powerpoint,bat, vbe, vbs, pif, ps1, hta, wsf, wsh, xz, rtf.
55. Rozwiązanie musi umożliwiać skanowanie bardzo dużych plików do wielkości 5GB oraz umożliwiać zablokowania plików powyżej wskazanego rozmiaru.

56. System powinien umożliwiać zarządzanie oparte o role / RBAC, w tym minimum rola administratora systemowego, analityka, API i pełnego administratora.
57. System musi umożliwiać przekazywanie próbek do analizy poprzez protokół ICAP lub poprzez REST API oraz poprzez konsolę zarzadzania.
58. Skanowanie plików antymalware musi uwzględniać następujące funkcjonalności:
    a) blokowanie plików skompresowanych z hasłem
    b) analiza wielokrotnie skompresowanych plików – co najmniej 40 poziomów zagnieżdżenia z możliwością zablokowania powyżej pewnego poziomu np. 10.
    c) limit ilości plików w archiwum – przekroczenie powinno skutkować zablokowaniem pliku – możliwość analizy nie mniej niż 50 tys. plików w archiwum.
    d) blokowanie nieznanych typów kompresji i w ogólności nieznanych formatów plików.
59. Funkcjonalność systemu:
    a) Wszystkie funkcje systemu dostępne z interfejsu graficznego powinny być również dostępne przez Remote API.
    b) Połączenia przez Remote API powinny być realizowane poprzez połączenie szyfrowane i wymagać uwierzytelnienia.
    c) Rozwiązanie musi umożliwiać rozbudowę o specjalizowane serwery sprzętowe tego samego producenta do wykonywania analizy dynamicznej próbek (sandboxing) bez przekazywania analizowanych danych na zewnątrz. Przez specjalizowany serwer należy rozumieć urządzenie zmodyfikowane sprzętowo i programowo przez producenta rozwiązania pod kątem wydajności i bezpieczeństwa. Ze względów bezpieczeństwa nie dopuszcza się rozwiązań wykorzystujących sandbox oparty o standardowe, ogólnodostępne silniki wirtualizacji (ang. hypervisor).
    d) Oferowane rozwiązanie musi umożliwiać integrację ze specjalizowanymi serwerami do analizy dynamicznej próbek (sandboxing) dostępnych w ofercie firm trzecich, tak aby możliwe było równoległe wykonanie detonacji na co najmniej 2 specjalizowanych serwerach analizy dynamicznej (sandboxing) pochodzących od dwóch niezależnych dostawców.
    e) Rozwiązanie jako zintegrowany system wykorzystujący 2 silniki AV oraz 2 specjalizowane systemy do detonacji próbek musi zapewniać jeden interfejs zapewniający przesłanie próbki do analizy, tj. wysłanie próbki musi być wykonane jeden raz, a dla żądania sprawdzenia zostanie zwrócona jedna odpowiedź z wynikiem analizy ze wszystkich komponentów rozwiązania. Odpowiedź musi być zwracana z centralnego systemu zarzadzania w jednym raporcie.
    f) Wydajność skanowania danych plikowych przez dwa silniki AV powinna być nie mniejsza niż 400Mb/s z wykorzystaniem do 16 sztuk vCPU dla jednego urządzenia.
    g) Wykorzystywana maksymalna przestrzeń dyskowa: 100 GB dla jednego urządzenia.
    h) Pamięć RAM maksimum wykorzystywane: 64 GB dla jednego urządzenia.
    i) Wymagane są minium dwa urządzenia skanujące pliki
60. Zaproponowane rozwiązanie systemowe musi posiadać **moduł raportujący**, spełniający następujące wymagania:
    a. Prekonfigurowana wirtualna maszyna pod środowisko VMWare ESX.
    b. Utwardzony system operacyjny bez zbędnych usług i kont poza tymi które są niezbędne do działania systemu.
    c. Wbudowana baza danych o wielkości co najmniej 2TB.
    d. Możliwość powiększenia bazy danych poprzez upgrade licencji.
    e. Graficzny interfejs zarządzania, dostępny przez przeglądarkę WWW, zabezpieczony protokołem TLS.

f. Predefiniowane raporty i możliwość dodawania własnych raportów.
g. Możliwość czyszczenia danych po założonym okresie np. 60 dni.
h. Generowanie raportów w formacie PDF i CSV w trybie na żądanie i według założonego harmonogramu.
i. Możliwość anonimizacji wybranych danych – minimum IP użytkownika i jego loginu.
j. Lokalni użytkownicy systemu i integracja z katalogiem LDAP.
k. Zarządzanie w oparciu o role, w tym możliwość definiowania własnych ról.
l. Wysyłanie powiadomień o działaniu systemu via SMTP.
m. Możliwość konfiguracji progów zajętości pamięci i dysków dla których następuje powiadomienie SMTP.
n. Możliwość uruchomienia serwera FTP(S) na którym będą składowane logi w nieprzetworzonej postaci (zanim trafią do bazy danych).
o. Interfejs programistyczny API.
p. Zarządzanie w oparciu o role, w tym możliwość definiowania własnych ról.
q. Minimalny zestaw raportów, które system powinien oferować:
    i. Najbardziej popularne kategorie URL.
    ii. Najbardziej popularne strony.
    iii. Zablokowane żądania per kategoria URL.
    iv. Zablokowane żądania per użytkownik.
    v. Zablokowane żądania per strona.
    vi. Lista użytkowników ściągających najwięcej danych.
    vii. Aktywność w serwisach społecznościowych.
    viii. Lista wykorzystywanych w firmie aplikacji webowych.
    ix. Lista użytkowników odwiedzających zabronione kategorie np. pornografię.
    x. Szczegółowy raport na temat danego użytkownika na podstawie IP lub nazwy użytkownika.
    xi. Lista zainfekowanych użytkowników, którzy łączą się ze znanymi serwerami C&C.
    xii. Czego szukają użytkownicy w Google, Bing itd.
    xiii. Wszystkie raport powinny dawać możliwość wygenerowania za żądany okres czasu – minimum 1 dzień, 30 dni, 90 dni, rok.
r. System musi pozwalać na automatyczne generowanie raportów na temat pracowników raportujących do danego menedżera.

61. Zaproponowane rozwiązanie systemowe musi posiadać **moduł zarządzający**, spełniający następujące wymagania:
    a. Prekonfigurowana wirtualna maszyna pod środowisko VMWare ESX.
    b. Utwardzony system operacyjny bez zbędnych usług i kont poza tymi które są niezbędne do działania systemu.
    c. Własna baza danych, bez potrzeby wysyłania ruchu na zewnątrz.
    d. Możliwość zarządzania systemami proxy.
    e. Możliwość zwiększenie liczby zarządzanych systemów przez upgrade licencji.
    f. Możliwość monitorowania systemów (filtrującego, skanującego i raportującego).
    g. Lokalni użytkownicy systemu i integracja z katalogiem LDAP.
    h. Zarządzanie w oparciu o role, w tym możliwość definiowania własnych ról.
    i. Możliwość integracji z systemem raportującym poprzez API – dane z modułu raportującego dostępne bezpośrednio w konsoli modułu zarządzającego.
    j. Konfigurowanie, zarzadzanie i instalacja polityki dla modułu filtrującego dla wielu urządzeń jednocześnie.
    k. Sprawdzanie spójności i synchronizacja polityk pomiędzy urządzeniami.
    l. Wersjonowanie polityk systemu proxy z możliwością porównania ze sobą różnych polityk znajdujących się w bazie konfiguracji.

m. W przypadku zmiany konfiguracji systemu proxy system musi wymuszać dodanie komentarza do zmiany.
n. Wersja polityki musi być związana z konkretnym użytkownikiem, który dokonał zmiany, a informacja o tym musi się znajdować w interfejsie graficznym.
o. Możliwość zautomatyzowania zadań poprzez skrypty i zaplanowane zadania.
p. Przechowywanie i udostępnianie plików na systemie zarządzania takich jak obrazy systemu operacyjnego czy pliki tekstowe.
q. Możliwość wykonania kopii zapasowej konfiguracji modułu filtrującego i skanującego.
r. Szyfrowanie backupu konfiguracji urządzeń.
s. Logowanie do systemu na bazie użytkowników lokalnych.
t. Logowanie do systemu z Active Directory, LDAP i Radius.
u. Synchronizacja czasu z serwerem NTP.
v. Monitorowanie przy pomocy SNMP poprzez odpytywanie bazy MIB.
w. Wysyłanie alarmów przy pomocy SNMP i SMTP.