Załącznik nr 1
Nr spr. 7/D/2022

Opis przedmiotu zamówienia

Modernizacja systemu zabezpieczeń środowiska teleinformatycznego poprzez wymianę klastra urządzeń sieciowych wraz z subskrypcjami oraz ich rozbudową.

I. Przedmiot zamówienia

1. Przedmiotem zamówienia jest modernizacja posiadanego systemu zabezpieczeń środowiska teleinformatycznego SPZZLO Warszawa-Żoliborz składającego się m.in. z klastra urządzeń Palo Alto Networks PA-3020 o poniższych numerach seryjnych:

L.p.	Opis urządzenia	Typ pracy	Numer seryjny
1	Palo Alto PA-3020	Klaster	001801023027
2	Palo Alto PA-3020		001801023151

2. W ramach ww. klastra urządzeń Zamawiający posiada licencje na aktywne subskrypcje:
   1) Partner enabled premium support year 1 renewal, PA-3020, 2 szt.
   2) Threat prevention subscription renewal for devices in HA pair, PA-3020, 2 szt.
   3) WildFire subscription renewal for devices in HA pair, PA-3020, 2 szt.
   4) PAN-DB URL filtering subscription renewal for devices in HA pair, PA-3020, 2 szt.

3. Modernizacja polegać będzie na:

   1) Dostawie i instalacji urządzeń PA-3220 tworzących klaster HA.
   2) Przeniesieniu konfiguracji z urządzeń PA-3020 na PA-3220 wraz z niezbędną aktualizacją oraz dostosowaniem do dostarczonych urządzeń.
   3) Aktywacji na dostarczonym klastrze urządzeń PA-3220 analogicznego zakresu licencji do wymienionych w pkt 2, ust. 1-3.
   4) Dostarczeniu dodatkowych licencji dla subskrypcji: PAN-PA-3220-DNS-HA2 (DNS Security) oraz PAN-PA-3220-ADVURL-HA2 (Advanced URL Filtering)
   5) Zapewnieniu konsultacji technicznych certyfikowanych przez producenta inżynierów w konfiguracji i administracji urządzeniami PA-3220 w wymiarze 36 godzin z możliwością wykorzystania w okresie 12 miesięcy od podpisania protokołu odbioru końcowego.

4. Posiadane obecnie przez Zamawiającego subskrypcje ważne są do 26 sierpnia 2022 roku. Przedmiot zamówienia powinien zostać zrealizowany w sierpniu 2022 roku, jednak nie później niż 26 sierpnia 2022 roku, tj. przed wygaśnięciem posiadanych przez Zamawiającego subskrypcji.

5. Wykonawca przygotuje harmonogram modernizacji oraz plan migracji, który przedstawi Zamawiającemu minimum 30 dni przed planowanym rozpoczęciem prac.
6. Wykonawca przygotuje dokumentację powykonawczą wykonanych prac w formie

elektronicznej edytowalnej, dokumentacja powinna zostać dostarczona na minimum 3 dni przed przystąpieniem do odbioru.

7. W ramach przedmiotu zamówienia Wykonawca dostarczy:

Lp.	Opis	Liczba sztuk
1	[PAN-PA-3220] Palo Alto Networks PA-3220 with redundant AC power supplies	2
2	[PAN-PA-3220-TP-HA2] Threat prevention subscription for device in an HA pair year 1, PA-3220	2
3	[PAN-PA-3220-ADVURL-HA2] Advanced URL Filtering Subscription, 1-year, PA-3220 HA Pair	2
4	[PAN-PA-3220-WF-HA2] WildFire subscription for device in an HA pair year 1, PA-3220	2
5	[PAN-PA-3220-DNS-HA2] DNS Security subscription for device in an HA pair year 1, PA-3220	2
6	[PAN-PA-2RU-RACK4] Palo Alto Networks PA-3220, PA-3250, and PA-3260 4 post rack mount kit	2
7	[PAN-SVC-BKLN-3220] Partner enabled premium support year 1, PA-3220	2
8	Konsultacje techniczne certyfikowanych przez producenta inżynierów w konfiguracji i administracji urządzeniami PA-3220 w wymiarze 36 godzin z możliwością wykorzystania w okresie 12 miesięcy od podpisania protokołu odbioru końcowego.	1

8. Wykonawca, w ramach Zamówienia dostarczy wsparcie techniczne (w tym gwarancję na urządzenia) ważne przez okres 12 miesięcy (z możliwością przedłużenia):
   1) Wsparcie techniczne świadczone będzie telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela.
   2) Wykonawca w ramach wsparcia technicznego Partner Enabled Premium Support zapewni:
      a) Pomoc techniczną świadczoną przez telefon, e-mail oraz w siedzibie Zamawiającego.
      b) Zgłaszanie usterek w dni robocze od 8.00 do 16.00.
      c) Zgłaszanie awarii całą dobę (odnosi się do awarii mających krytyczny wpływ na środowisko produkcyjne (np. odcięcie sieci), dla których nie są dostępne rozwiązania zastępcze.
      d) Czas reakcji przy zgłoszeniach awarii 2 godziny, przy usterkach 6 godzin.
      e) Czas przywrócenia funkcjonalności rozwiązania nastąpi w ciągu 24 godzin od momentu dokonania zgłoszenia awarii oraz 72 godziny od momentu zgłoszenia usterki.
   3) Czas przywrócenia funkcjonalności wynikającej z usterki w ciągu 72 godzin od momentu zgłoszenia. W przypadku zgłoszeń, których okres 72 godzin nie kończy się w dzień roboczy, naprawa nastąpi pierwszego dnia roboczego z zaliczeniem czasu realizacji w ostatni dzień roboczy (np. zgłoszenie przyjęte w piątek o godzinie 12.00 powinno zostać zrealizowane w poniedziałek godz. 12.00),
   4) Dostęp do nowych wersji oprogramowania.
   5) Aktualizację bazy ataków IPS.

6) Aktualizację definicji wykrywanych wirusów.
7) Aktualizację bazy kategorii stron WWW.
8) Aktualizację systemu WildFire.
9) Aktualizacja systemu DNS Security.
10) Nieograniczony dostęp do baz wiedzy i przewodników konfiguracyjnych oraz narzędzi diagnostycznych.

9. Wszelkie koszty usunięcia awarii bądź usterki (usług, części, sprzętu zastępczego i transportu) ponosi Wykonawca.
10. Wykonawca, w ramach Zamówienia dostarczy konsultacje techniczne certyfikowanych przez producenta inżynierów w konfiguracji i administracji urządzeniami PA-3220 w wymiarze 36 godzin z możliwością wykorzystania w okresie 12 miesięcy od podpisania protokołu odbioru końcowego. Konsultacje będą realizowane drogą e-mail, telefonicznie, zdalnie oraz w siedzibie Zamawiającego. Dotyczyć będą typowych zadań administracyjnych – konfiguracje, modyfikowanie polityk, aktualizacje itp.

***Awaria**
- awaria sprzętowa klastra PA-3220 w wyniku którego system nie realizuje swoich zdań.
- awaria programowa dowolnego modułu programowego, systemu operacyjnego czy mechanizmu inspekcji ruchu bądź dowolnego innego modułu bezpieczeństwa w wyniku którego system nie realizuje swoich zadań.

***Usterka**
- awaria sprzętowa jednego urządzenia PA-3220 nie powodująca przerwy w pracy systemu (drugie urządzenie PA-3220 pracuje prawidłowo).
- nieprawidłowość, która tylko w niewielkim stopniu wpływa na wybrane usługi o niestrategicznym znaczeniu dla Zamawiającego i dla której Zamawiający dopuści dłuższą procedurę wsparcia technicznego.

Kryteria równoważności w zakresie parametrów podstawowych, parametrów ochrony przed atakami oraz parametrów sprzętowych.

Wymagane parametry podstawowe

1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active - zmiana trybu pracy nie może wymagać poniesienia dodatkowych kosztów za sprzęt, licencje i oprogramowanie.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta.
3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
   a) routera (tzn. w warstwie 3 modelu OSI),
   b) mostu (tzn. w warstwie 2 modelu OSI),
   c) w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary),
   d) w trybie pasywnego nasłuchu kopii ruchu (sniffer/tap).
4. Zaoferowane rozwiązanie musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych, w pojedynczej logicznej instancji systemu.
5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.

6. Urządzenia firewall muszą posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
7. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać co najmniej 4000 znaczników VLAN.
8. Urządzenia firewall muszą wspierać protokół LACP.
9. Urządzenia firewall muszą, zgodnie z ustaloną polityką, prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (odpowiednio w warstwie L3, L4, L7).
10. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Muszą blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
11. Polityka zabezpieczeń firewall musi uwzględniać i umożliwiać jej określenie na podstawie:
    a) adresy IP źródłowe i docelowe,
    b) protokoły i usługi sieciowe,
    c) aplikacje,
    d) kategorie URL,
    e) użytkownicy aplikacji i grupy użytkowników,
    f) reakcje zabezpieczeń,
    g) logowanie zdarzeń (początek i koniec sesji),
    h) strefa bezpieczeństwa wejściowa i wyjściowa.
12. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów, z których aplikacja korzysta (założenie, że dana aplikacja może występować na każdym z dostępnych 65 tys. portów). Wymóg ten dotyczy również aplikacji typu P2P i IM.
    a) identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury udostępniane przez producenta i opracowane przez administratora systemu,
    b) urządzenia muszą wykrywać co najmniej 3300 predefiniowanych przez producenta aplikacji, w tym aplikacje tunelujące się w HTTP lub HTTPS,
    c) musi być możliwe ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio w GUI urządzenia (bez użycia zewnętrznych narzędzi),
    d) nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile,
    e) nie jest dopuszczalna kontrola aplikacji w modułach innych niż firewall (np. w module IPS lub innym module UTM, z użyciem sygnatur IPS),
    f) nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
13. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, wśród nich co mniej następujących typów: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i metadanych pliku.
14. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalna konieczność instalacji dedykowanego oprogramowania (tzw. klienta) na stacji, z której wykonywane jest zarządzanie Web GUI w celu zarządzania firewallem.
15. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć takowe dla minimum 30 użytkowników i systemów wykorzystujących API.
16. Dostęp do urządzeń i zarządzanie nimi muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). Oferowane rozwiązanie musi pozwalać na zdefiniowanie wielu administratorów systemu o różnych uprawnieniach.
17. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być

wspierane uwierzytelnianie za pomocą kluczy SSH, a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

18. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników, których ruch sieciowy jest kontrolowany i integrować się w tym zakresie z systemami:
    a) Active Directory,
    b) Terminal Services.
19. Polityka kontroli dostępu (zdefiniowana na urządzeniach firewall) musi precyzyjnie określać prawa dostępu użytkowników organizacji do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, mających wspólny adres IP źródłowy, ustalanie tożsamości również musi odbywać się transparentnie, bez konieczności interakcji z użytkownikiem.
20. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk wbudowany w urządzenie firewall) i analizowanie logów, korelowanie zbieranych informacji oraz budowanie raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, wykrytych zagrożeniach, filtrowaniu adresów URL, deszyfracji ruchu SSL.
21. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu firewall i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników we wskazanym okresie czasu.
22. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach, które są dynamicznie przypisywane w efekcie:
    a) reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
    b) poprzez interfejs API.
23. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku HTTP ustawionego przez web proxy i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję
24. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach w postaci maszyn wirtualnych (VM), ich adresach IP i etykietach (tagi) w środowisku VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
25. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6.
26. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
27. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT, rozdzielny od polityk bezpieczeństwa.
28. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
29. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów do innych systemów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.
30. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników i inspekcji zdeszyfrowanego połączenia (IPS, anti-wirus, filtracja URL, itd.) dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
31. Urządzenia firewall muszą posiadać sposób zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji bezpieczeństwa, rozdzielny od polityk bezpieczeństwa.
32. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takich przypadkach urządzenie musi umożliwiać blokadę sesji użytkownika.

33. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Informacja musi zawierać dane ułatwiające diagnostykę procesu deszyfracji m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie takiego logu.
34. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
35. Oferowane rozwiązanie musi posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta powinna stanowić automatyczne wyjątki od ogólnych reguł deszyfracji.
36. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
37. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością ograniczenia ilości jednoczesnych sesji na podstawie źródłowego lub docelowego adresu IP.
38. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma ruchu.
39. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania pakietów (tzw. routing-based VPN).
40. Dla IKE wymagane jest wsparcie minimum standardów: AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
41. Dla IPsec wymagane jest wsparcie minimum standardów: AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
42. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego z chronionej sieci w celu blokowania tuneli SSH.

Wymagane specjalistyczne parametry ochrony przed atakami

43. Urządzenia firewall muszą posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (tzw. IPS/IDS). Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent oferowanego systemu zabezpieczeń.
44. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby zaszła taka potrzeba.
45. Urządzenia firewall muszą posiadać funkcję ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu.
46. Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/reguła polityki na urządzeniu dla minimum następujących protokołów komunikacji: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na dobę i pochodzić od tego samego producenta co oferowany system firewall.
47. Urządzenia firewall muszą posiadać funkcję anty-spyware. Baza sygnatur takich ataków musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co oferowany system firewall.
48. Musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
49. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
50. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per całe urządzenie lub jego część (np. per interfejs sieciowy, per strefa bezpieczeństwa).
51. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

52. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C (command and control) oraz ostatnio zarejestrowane domeny.
53. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.
54. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznego systemu analizy (tzw. sandbox) w celu ochrony przed zagrożeniami typu zero-day plików różnych typów, co najmniej: Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, BAT, HTA.
    a) usługa sandbox musi pochodzić od tego samego producenta co oferowany system firewall,
    b) na podstawie przeprowadzonej analizy, sandbox musi udostępniać dla systemu firewall sygnatury nowo wykrytych złośliwych plików oraz adresów IP, DNS i ewentualnej komunikacji zwrotnej (callback) powiązanych ze złośliwym plikiem, wykrytych w czasie jego analizy,
    c) maksymalny interwał aktualizacji sygnatur nie może przekraczać 2 godzin.
55. Administrator musi mieć możliwość konfiguracji jakiego rodzaju typy plików z listy wspieranych przez usługę sandbox zostaną wysłane do analizy.
56. Urządzenia firewall muszą realizować ochronę DNS w zakresie:
    a) wykrywania i blokowania zapytań do domen złośliwych (baza domen musi mieć co najmniej 10 milionów wpisów),
    b) możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing),
    c) wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA),
    d) wykrywanie domen dynamicznych Dynamic DNS,
    e) wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych.
57. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
58. Urządzenia firewall muszą posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) działających bezpośrednio na oferowanych urządzeniach. Reguły ML muszą być aktualizowane dynamicznie przez producenta oferowanych urządzeń. Wykrywanie za pomocą algorytmów ML musi odbywać się lokalnie na urządzeniu, jako uzupełnienie innych funkcji ochrony przed atakami bazujących na sygnaturach anty-wirus oraz funkcji filtrowania URL umożliwiając zmniejszenie ryzyka wystąpienia tzw. "pacjenta zero" (zainfekowany host w czasie kiedy nie były jeszcze dostępne sygnatury ataku). Wymagane jest realizowanie funkcji wykrywania za pomocą ML (Machine Learning) co najmniej dla następujących danych:
    a) złośliwe pliki wykonywalne (tzw. PE i DLL),
    b) złośliwe skrypty PowerShell,
    c) złośliwe strony web realizujące ataki phishing,
    d) złośliwe skrypty JavaScript.
59. Urządzenia firewall muszą posiadać możliwość określenia tzw. konfiguracji kandydackiej (przez API, GUI oraz CLI), którą można dowolnie edytować na urządzeniu, bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia, do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. Konfiguracja kandydacka musi być wspierana przez minimum 7 dni. W tym:
    a) możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwolenie im na zatwierdzanie i cofanie zmian, których są autorami,
    b) możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
60. Urządzenia firewall muszą umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w GUI urządzenia firewall, nie może wymagać korzystania z CLI lub z rozwiązań zewnętrznych.
61. Urządzenia firewall muszą posiadać możliwość automatycznego zbierania i analizowania informacji syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia.

Parametry sprzętowe

62. Zaoferowane rozwiązanie będzie pracowało w trybie klastra HA - wymagana jest dostawa 2 sztuk urządzeń firewall
    a) urządzenia muszą posiadać dedykowane porty do komunikacji wewnątrz klastra - porty te nie wliczają się do niżej wymienionych ilości interfejsów analizujących ruch sieciowy
63. Każde z dostarczonych urządzeń firewall musi być wyposażone w minimum:
    a) 12 wbudowanych interfejsów 10/100/1000 Ethernet (RJ45)
    b) 4 wbudowane porty 1GE pozwalające na obsadzenie modułami SFP 1GE
    c) 4 wbudowane gniazda elastyczne Ethernet pozwalające na obsadzenie modułami SFP 1GE oraz SFP+ 10GE. Jeżeli urządzenie nie wspiera gniazd elastycznych musi posiadać 4 gniazda SFP 1GE plus 4 gniazda SFP+ 10GE.
64. Każde z urządzeń musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 i w co najmniej jeden dedykowany port zarządzający Ethernet RJ45 10/100/1000.
65. Urządzenie musi być wyposażone w zasób dyskowy SSD o pojemności minimum 240 GB na potrzeby systemu operacyjnego i logów.
66. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
    a) minimum 4.5 Gbps dla rozpoznawania i kontroli aplikacji,
    b) minimum 2.2 Gbps dla transakcji o wielkości 64KB przy wykorzystaniu rozpoznawania i kontroli aplikacji i jednocześnie przy włączonych funkcjach bezpieczeństwa: włączone wszystkie dostępne sygnatury IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,
    c) minimum 50 tys. nowych sesji na sekundę,
    d) minimum 1 mln równoległych sesji.
67. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
68. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż:
    a) 10 tys. reguł polityki bezpieczeństwa,
    b) 3 tys. reguł NAT,
    c) 200 stref bezpieczeństwa,
    d) 150 profili bezpieczeństwa, które określają reguły wykrywania zagrożeń i które następnie mogą być użyte jako parametr w definicji reguły polityki bezpieczeństwa.
69. Urządzenie musi umożliwiać wysyłanie kopii zdeszyfrowanego ruchu SSL na wskazany interfejs urządzenia celem poddania go dodatkowej analizie przez inne produkty bezpieczeństwa.