SPECYFIKACJA TECHNICZNA SIECI TRANSMISJI DANYCH I DOSTĘPU DO INTERNETU DLA URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA MAZOWIECKIEGO W WARSZAWIE

Osobą wyznaczoną przez Zamawiającego do sprawdzenia warunków technicznych dla łączy i usług dostarczanych do placówek i jednostek Zamawiającego w zakresie usług transmisji danych i dostępu do Internetu jest Pan Arkadiusz Jedynak, tel. 22 5979334, mail: arkadiusz.jedynak@mazovia.pl

Struktura dokumentu:

I. PRZEDMIOT ZAMÓWIENIA:

I.1. Sieć IP VPN MPLS.
I.2. Łącza internetowe.
I.3. Punkty dostępowe Wifi.
I.4. Ochrona oraz mitygacja przed atakami typu DDoS.
I.5. System zaawansowanej ochrony dla stacji końcowych i serwerów Zamawiającego.
I.6. Centralny system chronionego, nadzorowanego dostępu do sieci Internet oraz zasobów publikowanych w Internecie przez Zamawiającego.

I.1. SIEĆ IP VPN MPLS

1. Przedmiotem Zamówienia jest usługa Wirtualnej Sieci Prywatnej o topologii Full Mesh, zbudowanej na bazie wydzielonej operatorskiej sieci MPLS Wykonawcy, odseparowanej od sieci Internet i opartej o łącza kablowe (preferowane światłowodowe). Dostarczona przez Wykonawcę sieć WAN ma zapewnić chroniony, nadzorowany dostęp do zasobów Internetowych dla poszczególnych Placówek oraz zapewnić chroniony, nadzorowany dostęp dla użytkowników Internetu do publikowanych przez Zamawiającego zasobów.

2. Ze względu na przyjętą politykę bezpieczeństwa sieci Zamawiający nie dopuszcza stosowania radiowych łączy dostępowych. Wymóg świadczenia usług przez łącza kablowe z wyłączeniem technologii radiowej uzasadnione jest jego potrzebami wynikającymi z charakteru wykonywanych zadań, w tym statusu informacji przetwarzanych w systemach informatycznych Zamawiającego.

3. Wszystkie placówki zdefiniowane w Tabeli 1 - muszą zostać dołączone do sieci VPN łączami symetrycznymi o gwarantowanych przepływnościach portów, zgodnie z poniższą tabelą:

LP	Nazwa placówki	Adres placówki	Prędkość portu dostępowego sieci VPN Zamawiającego
1	Skoczylasa	03-469 Warszawa, ul. Skoczylasa 4	1000/1000 Mbps
2	Jagiellońska	03-719 Warszawa, ul. Jagiellońska 26	1000/1000 Mbps
3	Kłopotowskiego 5	03-718 Warszawa, ul. Kłopotowskiego 5	300/300 Mbps
4	Bankowy	00-142 Warszawa, Plac Bankowy 3/5	300/300 Mbps
5	Kłopotowskiego 22	03-717 Warszawa, ul. Kłopotowskiego 22	300/300 Mbps
6	Solidarności	03-402 Warszawa, ul. Solidarności 61	300/300 Mbps
7	Kijowska	03-743 Warszawa, ul. Kijowska 10A	300/300 Mbps
8	Chrobrego	02-479 Warszawa, ul. Chrobrego 29	100/100 Mbps
9	Ciechanów	06-400 Ciechanów ul. Wodna 1	100/100 Mbps
10	Ostrołęka	07-410 Ostrołęka ul. Piłsudskiego 38	100/100 Mbps
11	Piaseczno	05-500 Piaseczno ul. Puławska 38	100/100 Mbps
12	Płock	09-402 Płock ul. Kolegialna 19	100/100 Mbps
13	Radom	26-600 Radom ul. Kościuszki 5a	100/100 Mbps
14	Siedlce	08-110 Siedlce ul. Wiszniewskiego 4	100/100 Mbps
15	Wołomin	05-200 Wołomin ul. Miła 3	100/100 Mbps
16	Żyrardów	96-300 Żyrardów ul. 1 Maja 17	100/100 Mbps

Tabela 1. Specyfikacja łączy dostępowych VPN

4. Dodatkowo pomiędzy wskazanymi niżej placówkami musi zostać zestawione łącze:
   a) Ethernet 4 Gbps:
      pomiędzy: Warszawa, ul. Skoczylasa 4 – Warszawa, ul. Jagiellońska 26,
      zakończone interfejsami optycznymi SM;
   b) Ethernet 1 Gbps:
      pomiędzy: Warszawa, ul. Kijowska 10A – Warszawa, ul. Mycielskiego 21.

Wymagania dotyczące sieci IP VPN MPLS

1. Wykonawca zakończy łącza dostępowe we wszystkich lokalizacjach Zamawiającego stosownymi modemami oraz routerami, które będą podlegały zarządzaniu i serwisowaniu przez Wykonawcę oraz Wykonawca udostępni podgląd pracy routerów w zakresie interfejsów (w opcji tylko do odczytu).
2. Wykonawca zapewni logiczne i fizyczne sieci WAN z łączami internetowymi będącymi przedmiotem zamówienia.
3. Punkt styku sieci lokalnej Zamawiającego i routerów Wykonawcy będzie zgodny ze standardem IEEE 802.3u (styk RJ45);

4. W każdej Placówce musi zapewnić urządzenie sieciowe będące zakończeniem łącza WAN z funkcjonalnością:
   a. DHCP, DHCP Relay,
   b. Filtrowanie pakietów za pomocą list dostępu
   c. NAT statyczny,
   d. routing statyczny
   e. routing dynamiczny
5. Zamawiający wymaga, aby routery dostarczone przez Wykonawcę były przeznaczone do montażu w standardowej szafie typu Rack 19” Zamawiającego.
6. Wykonawca dostarczy narzędzie monitorujące pracę sieci VPN Zamawiającego oparte o przeglądarkę internetową dowolnego dostawcy.
7. Zamawiający wymaga, aby dla każdej z lokalizacji zostały zapewnione mechanizmy kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej. Przez mechanizmy kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej Zamawiający rozumie wykorzystanie reguł firewall, access-list, ustawianie routingu itp.

I.2. ŁĄCZA INTERNETOWE

1. Wymagane medium transmisyjne: łącze światłowodowe.
2. Symetryczny dostęp do sieci Internet o parametrach CIR = EIR w placówkach wymienionych w Tabeli 2.

LP	Nazwa placówki	Adres placówki	Prędkość
1	Skoczylasa (dostępowe)	03-469 Warszawa, ul. Skoczylasa 4	500/500 Mbps
2	Skoczylasa (usługowe)	03-469 Warszawa, ul. Skoczylasa 4	500/500 Mbps
3	Jagiellońska (dostępowe)	03-719 Warszawa, ul. Jagiellońska 26	500/500 Mbps

Tabela 2. Specyfikacja łączy dostępowych do Internetu

3. Zamawiający oczekuje, że łącza wymienione w pkt. 2 będą odseparowane od siebie fizycznie i logiczne, z niezależną adresacją. Warunek ten zostanie spełniony przez zapewnienie oddzielnego przyłącza budynkowego, oddzielnych światłowodów oraz oddzielnych urządzeń końcowych.
4. Zapewnienie minimum 16 publicznych adresów IP dla każdego z łącz wymienionych w pkt. 2.
5. Zakończenie łączy u Zamawiającego zgodne ze standardem IEEE 802.3u (styk RJ45).
6. Zapewnienie usługi zapasowego serwera DNS (Secondary DNS).
7. Zapewnienie usługi serwera RevDNS.
8. Możliwość wsparcia dla protokołu BGP v4.0 w czasie trwania umowy.
9. Wykonawca zagwarantuje SLA o następujących parametrach:
   a) Godzinową, roczną dostępność placówki na poziomie co najmniej 99,6%.
   b) Usunięcie awarii lub uszkodzenia placówki w przeciągu max. 8 godzin zagwarantowane przez cały okres świadczenia usługi. Usunięcie awarii lub usterki będzie poprzedzone powiadomieniem ze strony Wykonawcy dedykowanej osoby/osób ze strony Zamawiającego o podjętych działaniach naprawczych.
10. Dopuszczalna przerwa w łączności w momencie uruchomienia usługi przy zmianie

operatora/medium 4 godziny w godzinach w czasie od 18.00 do 6.00.

11. Planowane przerwy techniczne w dni robocze od 18.00 do 6.00 nie dłużej niż 4 godziny.

I.3. PUNKTY DOSTĘPOWE WIFI.

1. W placówce Warszawa, ul. Jagiellońska 26, we wskazanych przez Zamawiającego miejscach, Wykonawca zainstaluje i uruchomi min. 5 punktów Wifi (sale konferencyjne: parter oraz III piętro; pomieszczenia VIP na III i IV piętrze).
2. Wszystkie punkty Wifi mają realizować usługę w ramach jednej sieci WLAN.
3. Sieć Wifi oraz wewnętrzna sieć LAN Zamawiającego muszą być odseparowane fizycznie i logicznie.
4. Sieć Wifi musi zapewnić dostęp do Internetu przez niezależne łącze dostępowe w stosunku do łączy zdefiniowanych w **punkcie I.2. Łącza internetowe.** Zamawiający oczekuje separacji fizycznej i logicznej.
5. Sieć Wifi musi zapewniać dostęp do Internetu z min. prędkością 100/100 Mbps.
6. Dostęp do sieci Wifi musi być zabezpieczony hasłem autoryzującym.
7. Zamawiający wymaga dostępu do panelu zarządzania urządzeń AccessPoint dla wskazanych po stronie Zamawiającego osób, w celu definiowania kluczy dostępu do sieci Wifi oraz monitorowania podłączonych urządzeń, w tym blokowania klientów.
8. Zamawiający oczekuje zapewnienia wymaganej prawnie retencji danych dla sieci Wifi.

W celu zrealizowania podstawowego założenia zamówienia, tzn. ochrony i nadzoru, Zamawiający oczekuje dostarczenia, wdrożenia oraz utrzymania przez Wykonawcę następujących elementów.

I.4. Ochrona oraz mitygacją przed atakami typu DDoS.

I.5. System zaawansowanej ochrony dla stacji końcowych i serwerów Zamawiającego.

I.6. Centralny system chronionego, nadzorowanego dostępu do sieci Internet oraz zasobów publikowanych w Internecie przez Zamawiającego.

I.4. OCHRONA ORAZ MITYGACJA PRZED ATAKAMI TYPU DDOS

W ramach usługi dostępu do Internetu należy zapewnić ochronę przeciw atakom Distributed Denial of Service (DDoS) typu wolumetrycznego.

W celu wykrycia ataków system Wykonawcy powinien monitorować sieć Wykonawcy i analizować strumienie danych z wykorzystaniem protokołu przepływu np. Net Flow.

System zabezpieczeń ma być umiejscowiony w sieci Wykonawcy i być przez niego w całości zarządzany. Ma on umożliwić ochronę przed atakami DDoS na adresację IPv4 Zamawiającemu do 10 Gbps. Adresację IPv4 zapewnia Wykonawca.

Po wykryciu ataku ruch zainfekowany ma zostać przekierowany do specjalnego Centrum Przeciwdziałania Atakom DDoS („Scrubbing Center") znajdującego się w sieci Wykonawcy. Po odfiltrowaniu ruchu niepożądanego, ruch oczyszczony jest kierowany ponownie do Klienta za pomocą np. . FlowSpec, tunelu GRE.

Ochrona powinna bazować na różnych rodzajach mechanizmów detekcji, w tym na:

– przekraczaniu progów dla określonych typów pakietów i protokołów,

– analizie profilu ruchu Klienta wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu,

– sygnaturach.

Ochrona przeciw atakom Distributed Denial of Service (DDoS) ma obejmować:

– monitorowanie ruchu w czasie rzeczywistym, w celu identyfikacji typu i natury ataku,

– powiadamianie Klienta o podejrzeniu wystąpienia ataku,

– rozpoczęcie usuwania ataku w porozumieniu z Klientem (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia),

– modyfikację zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy.

Mitygacja (filtrowanie) ataków:

1. Usługa zapewnia filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP
2. Usługa zapewnia odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI.
3. Usługa zapewnia filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne.
4. Usługa zapewnia filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne
5. Usługa chroni przed atakami ze „spoofowanymi" (udawanymi) adresami źródłowymi IP poprzez autentykację sesji TCP, zapytań DNS oraz zapytań HTTP.
6. Usługa zapewnia filtrowanie nieprawidłowych zapytań DNS
7. Usługa umożliwia ograniczenia zapytań DNS do zadanej wartości zapytań/sek.
8. Usługa zapewnia do 5-ciu filtrów opartych o wyrażenia regularne definiujących zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS.
9. Usługa zapewnia filtrowanie nieprawidłowych zapytań HTTP.
10. Usługa zapewnia blokowanie ruchu od stacji końcowych przekraczających progi dla operacji HTTP na sekundę per serwer lub per URL.
11. Usługa zapewnia do 5-ciu filtrów opartych o wyrażenia regularne definiujących zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań HTTP.
12. Usługa zapewnia filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP.
13. Usługa powinna zapewniać ochronę przez atakami typu „slow Lories", poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu.
14. Usługa zapewnia ochronę przez atakami typu „slow Lories", poprzez resetowanie sesji TCP której opaktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu.
15. Usługa wykrywa ruch kierowany z serwerów CDN proxy i stosować algorytmy filtrowania na podstawie oryginalnego źródła ruchu.
16. Usługa zapewnia wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS które są poza sekwencją.

17. Usługa zapewnia blokowane sesji jeżeli podczas negocjacji SSL/TLS klient zażąda nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. Próg dla tych wartości jest konfigurowalny.
18. Usługa zapewnia wykrywanie i rozłączanie sesji jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie.
19. Usługa zapewnia blokowanie ruchu ze stacji dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL.
20. Usługa monitoruje negocjację SSL dla wszystkich portów na których mogą być stosowane aplikacje zabezpieczone protokołem TLS: HTTPS, SMTP, IMAP4, POP, LDAP, IRC, NNTP, TELNET, FTP i SIP.
21. Usługa chroni przed atakami pochodzącym od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP.
22. Usługa chroni przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe są definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.
23. Usługa pozwala na uruchamianie mitygacji w celu nauczenia się systemu wartości typowych ruchu, które następnie mogą być wykorzystywania do właściwego ustawiania progów dla algorytmów mitygacji

Głównym parametrem systemu ochrony przeciw DDOS jest maksymalny czas, w jakim do Zamawiającego zostanie wysłane powiadomienie o zaistnieniu potencjalnego ataku na monitorowane usługi. Czas ten liczony jest od wystąpienia zdarzenia i wynosi on 15 minut. Sposób powiadomienia ustalony zostanie na etapie realizacji usługi.

Wykonawca zapewni poprzez stronę www dostęp do panelu umożliwiającego prezentację statystyk pochodzących z systemu ochrony przed atakami DDoS. Dostęp zostanie udzielony uprawnionym po stronie Zamawiającego osobom (przewiduje się 4 osoby).

I.5. SYSTEM ZAAWANSOWANEJ OCHRONY DLA STACJI KOŃCOWYCH I SERWERÓW

Wykonawca dostarczy, wdroży oraz utrzyma zaawansowany systemu ochrony 1400 stacji końcowych użytkowników oraz serwerów zgodnie z poniższymi wymaganiami funkcjonalnymi:

System musi zapewniać ochronę dla co najmniej 1400 chronionych stacji końcowych (Windows) przez okres 3 lat oraz musi przechowywać logi generowane przez agentów przez okres określony przez Zamawiającego (obecnie 120 dni; parametr ten musi być konfigurowalny przez Zamawiającego).

1. System musi składać się z centralnej konsoli zarządzania chronionymi systemami, zarządzania incydentami i raportowania (w skrócie konsoli) oraz oprogramowania uruchomionego na stacjach końcowych, serwerach i urządzeniach mobilnych tzw. agenta
2. Agent musi umożliwiać instalację i uruchomienie na następujących platformach:
   a. Windows 10, Windows 8.1, Windows Embedded 8.1
   b. Microsoft Windows Server 2012, 2012 R2, 2016, 2019
4. Agent musi działać równolegle z istniejącymi w organizacji rozwiązaniami zabezpieczeń stacji końcowych (np. AntyVirus, HIPS, itp.) w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwym oprogramowaniem.
5. Agent musi posiadać możliwość instalacji i uruchomienia na stacjach roboczych z nie więcej niż 2GB pamięci RAM
8. Agent musi integrować się z mechanizmem Windows Security Center oraz umożliwiać użytkownikowi manualne przeskanowanie wybranego pliku.
9. Agent musi posiadać opcję komunikacji z systemem za pośrednictwem proxy webowego
10. Wszystkie mechanizmy ochrony system musi realizować metodami, które nie wykorzystują bazy sygnatur. Ochrona bezsygnaturowa jest wymagana w celu zapewnienia ochrony przed nowymi atakami, które nie zostały opisane przy pomocy sygnatur, czyli tzw. atakami dnia zerowego.
11. System musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla ochranianego przez agenta systemu z rozróżnieniem reguł obowiązujących w sieci wewnętrznej i poza siecią wewnętrzną.
12. System musi posiadać możliwość zarządzania zasadami szyfrowaniem dysków systemu ochranianego przez agenta.
13. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB systemu ochranianego przez agenta w zakresie:
    a. blokowania podłączenia czytników CD-ROM
    b. blokowania podłączania zewnętrznych nośników pamięci flash
    c. blokowania podłączania urządzeń przenośnych (typu odtwarzacze mp3, aparaty fotograficzne)
    d. tworzenia listy wyjątków od reguły blokowania z określeniem trybu dostępu (tylko odczyt, odczyt i zapis) i atrybutów urządzenia obejmujących producenta i nr seryjny
    e. dodawania zablokowanych urządzeń tymczasowo do listy wyjątków na określony okres czasu z określeniem trybu dostępu (tylko odczyt, odczyt i zapis)
14. System musi posiadać mechanizmy ochrony przed wykorzystywaniem znanych i

nieznanych luk bezpieczeństwa oprogramowania (ochrona anty-exploit).

15. System na potrzeby ochrony anty-exploit nie może stosować technik analizy exploitów wykorzystujących w jakikolwiek sposób zasoby sprzętowe na potrzeby lokalnego środowiska symulacyjnego typu sandbox lub zwirtualizowany kontener.
16. System w przypadku wykrycia techniki ataku ukierunkowanej na podatną aplikację w celu zablokowania ataku musi zatrzymać proces atakowanej aplikacji oraz zebrać zestaw danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą proces wraz parametrami i znacznik czasowy
17. System w zakresie ochrony anty-exploit musi zapewniać co najmniej:
    a. ochronę przed atakami wykorzystującymi technikę Return Oriented Programming
    b. ochronę przed atakami wykorzystującymi technikę Structure Exception Handler
    c. mitygację ataków z wykorzystaniem techniki Address Space Layout Randomization oraz Date Execution Prevention
    d. ochronę przed atakami wykorzystującymi technikę Null Dereference
    e. ochronę przed atakami wykorzystującymi kompilatory typu JIT
    f. ochronę przed atakami wykorzystującymi funkcje systemowe do omijania mechanizmu Data Execution Prevention i Address Space Layout Randomization
    g. ochronę przed podniesieniem uprawnień
    h. ochronę przed nadużyciami Asynchronous Procedure Calls
    i. ochronę przed enumeracją pamięci procesu
18. System musi obsługiwać sandboxing, czyli możliwość analizy próbki potencjalnie złośliwego oprogramowania w dedykowanym środowisku celem obserwacji jego zachowań i podjęcia decyzji o szkodliwości próbki w zakresie co najmniej:
    a. detekcji i usunięcia mechanizmów mających na celu zaciemnienie kodu binarnego próbki (ang. obfuscation / packing)
    b. analizy statycznej próbki i wykorzystania metadanych próbki w połączeniu z algorytmami uczenia maszynowego
    c. analizy dynamicznej, gdzie próbka jest uruchamiana a jej zachowanie obserwowane w środowisku wirtualnym
    d. analizy dynamicznej, gdzie próbka jest uruchamiana a jej zachowanie obserwowane w środowisku fizycznym
    e. obsługi następujących systemów operacyjnych w środowisku analizy: Windows 10 64-bit.
19. Usługa sandbox wykorzystywana przez system musi być realizowana przez sandbox lokalny lub przez sandbox chmurowy zlokalizowany na terenie Unii Europejskiej. W przypadku stosowania sandboxa lokalnego należy przewidzieć rozwiązanie pozwalające na analizę co najmniej 500 próbek na godzinę (VM sandboxing)
20. System dla platform Windows musi realizować ochronę przed uruchomieniem złośliwego oprogramowania co najmniej poprzez:
    a. sandboxing
    b. lokalną statyczną analizę w połączeniu z uczeniem maszynowym
    c. ochronę plików współdzielonych bibliotek DLL
    d. ochronę przed złośliwymi makrami w dokumentach pakietu Microsoft Office
    e. identyfikowanie ataków poprzez śledzenie i grupowanie pozornie niegroźnych

pojedynczych zdarzeń w systemie operacyjnym

f. uruchamianie nieznanych plików tylko jeśli są one cyfrowo podpisane przez zaufanych dostawców oprogramowania
g. kontrolę procesów potomnych
h. blokowanie wykonywania plików z określonych lokalizacji takich jak co najmniej: ścieżka, folder sieciowy, zewnętrzny nośnik pamięci
i. periodyczne i zautomatyzowane skanowanie
j. ochronę plików wykonywanych w formacie PE

24. System musi oferować ochronę przed złośliwym oprogramowaniem szyfrującym dyski (tzw. Ransomware)
25. System musi oferować opcję tworzenia wyjątków dla automatycznych werdyktów systemu z wykorzystaniem unikalnego identyfikatora pliku obliczanego funkcją skrótu np. SHA-256
26. System musi posiadać konsolę formie aplikacji webowej dostępną przy pomocy przeglądarki internetowej
27. Dostęp do konsoli musi być realizowany z zapewnieniem poufności, integralności przesyłanych danych oraz uwierzytelnienia serwera
28. Konsola musi obsługiwać dwuskładnikowe uwierzytelnienie administratorów
29. System musi oferować możliwość zabezpieczenia agenta przed odinstalowaniem przy pomocy hasła oraz wymuszenie zdalnego odinstalowania i zdalnej aktualizacji
30. Konsola systemu musi być w całości utrzymywana przez producenta systemu w zakresie dostarczenia mocy obliczeniowej, wysokiej dostępności, przestrzeni na przechowywanie logów/zdarzeń i aktualizacji
31. Wszystkie dane gromadzone przez system muszą być przechowywane na terenie Unii Europejskiej
32. Konsola systemu musi posiadać możliwość budowy dopasowanych kokpitów (inaczej dashboardów) per administrator, w ramach których prezentowane będą co najmniej:
    a. liczba aktywnych i nieaktywnych agentów
    b. liczba agentów w funkcji platformy tj. Windows
    c. liczba agentów w funkcji wersji oprogramowania
    d. liczba chronionych systemów w funkcji wersji aktualizacji silników inspekcyjnych
    e. top 10 chronionych systemów powiązanych z największą liczbą incydentów
    f. liczba incydentów w funkcji istotności incydentu, gdzie istotność incydentu to np. niska, wysoka, krytyczna
    g. liczba incydentów w funkcji rodzaju zagrożenia, gdzie rodzaj zagrożenia to co najmniej malware i exploit
33. Konsola systemu musi posiadać funkcję wyszukiwania z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, adres IP, funkcja skrótu, domena
34. Konsola musi obsługiwać przypisywanie użytkownikom konsoli różnego zakresu dostępu bazującego na rolach (tzw. Role Based Access Control) a w tym co najmniej musi umożliwiać przypisanie co najmniej następujących ról:
    a. nieograniczony dostęp w trybie zmiany do wszystkich elementów konfiguracji systemu
    b. dostęp tylko do elementów konfiguracji powiązanych z instalacją agenta
    c. dostęp tylko do obsługi incydentów
35. System musi posiadać funkcje budowania dopasowanych do potrzeb raportów w formacie

PDF udostępniając co najmniej następującą bibliotekę elementów:

a. liczba chronionych systemów w funkcji platformy tj. Windows
b. liczba chronionych systemów w funkcji aktywnych i nieaktywnych agentów
c. liczba chronionych systemów w funkcji wersji agenta
d. liczba chronionych systemów w funkcji wersji aktualizacji silników inspekcyjnych
e. liczba incydentów w funkcji statusu incydentu, gdzie status to np. nowy, rozwiązany, przetwarzany
f. liczba incydentów w funkcji istotności incydentu, gdzie istotność incydentu to np. niska, wysoka, krytyczna
g. liczba incydentów w funkcji rodzaju zagrożenia, gdzie rodzaj zagrożenia to co najmniej malware i exploit
h. top 10 chronionych systemów powiązanych z największą liczbą incydentów

36. System musi umożliwiać określenie harmonogramu, zgodnie z którym będą generowane raporty wraz z opcją wskazania adresu email, na który wygenerowany raport ma zostać wysłany
37. System musi umożliwiać integrację z Active Directory
38. System musi umożliwiać przekazywanie logów do zewnętrznych serwerów SYSLOG zapewniając poufność transmisji z wykorzystaniem TLS
39. System musi umożliwiać integrację z platformą komunikacyjną Slack w celu przekazywania powiadomień
40. System musi umożliwiać filtrowanie logów i powiadomień wysyłanych przy pomocy SYSLOG i Slack co najmniej przy pomocy atrybutu istotność zdarzenia
41. System musi umożliwiać wysyłanie powiadomień na wskazane adresy email
42. System musi umożliwiać przygotowywanie pakietów instalacyjnych agenta
43. System musi umożliwiać zdalne pobranie pakietu supportowego wykorzystywanego do diagnostyki agenta
44. System musi umożliwiać nawiązanie połączenia terminalowego z linią poleceń do system chronionego przez agenta, przy czym musi istnieć możliwość wyłączenia tej funkcji w trakcie instalacji agenta bez możliwości jej późniejszej aktywacji z konsoli systemu
45. System musi umożliwiać pobieranie plików z systemu chronionego przez agenta, przy czym musi istnieć możliwość wyłączenia tej funkcji w trakcie instalacji agenta bez możliwości jej późniejszej aktywacji z konsoli systemu
46. System musi umożliwiać grupowanie systemów z zainstalowanym agentem przy pomocy co najmniej typu systemu (serwer, stacja robocza, urządzenie mobilne), systemu operacyjnego, domeny (dotyczy systemów Windows) i członkostwa w grupie Active Directory (dotyczy systemów Windows) i przypisywania do tak zdefiniowanej grupy wybranej konfiguracji agenta
47. System musi posiadać opcję weryfikacji, czy agent posiada łączność z konsolą
48. System musi odkładać logi audytowe śledzące wszystkie zmiany konfiguracyjne i akcje administratorów wykonywane za pośrednictwem konsoli
49. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień agenta i przypisanie ich do grupy chronionych systemów:
    a. maksymalna przestrzeń na logi
    b. ukrycie ikony w zasobniku systemowym
    c. włączenie i wyłączenie dostępu do zdalnej linii poleceń chronionego systemu

d. włączenie i wyłączenie powiadomień o nawiązaniu połączenia do zdalnej linii poleceń chronionego systemu
e. włączenie i wyłączenie powiadomień użytkownika
f. dopasowanie treści powiadomień użytkownika
g. określenie hasła deinstalacji
h. ochrona przed wyłączeniem procesów agenta
i. włączenie i wyłączenie automatycznej aktualizacji agenta
j. włączenie i wyłączenie uploadu w sieci komórkowej

50. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień ochrony przed wykorzystaniem luk bezpieczeństwa w oprogramowaniu (ochrony anty-exploit) i przypisanie ich do grupy chronionych systemów:
    a. włączenie i wyłączenie ochrony dla procesów przeglądarek Internetowych
    b. włączenie i wyłączenie ochrony dla procesów systemowych
    c. włączenie i wyłączenie ochrony przed nadużyciami wywołań systemowych
    d. włączenie i wyłączenie ochrony dla procesów użytkownika
51. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień ochrony przed wykonywaniem złośliwego oprogramowania (ochrona anty-malware) i przypisanie ich do grupy chronionych systemów:
    a. włączenie i wyłączenie identyfikowania ataków poprzez śledzenie i grupowanie pozornie niegroźnych pojedynczych zdarzeń w systemie operacyjnym
    b. włączenie i wyłączenie ochrony przed atakami typu ransomware
    c. włączenie i wyłączenie ochrony przez wykrywanie złośliwych procesów potomnych
    d. włączenie i wyłączenie wykrywania złośliwych plików wykonywalnych i określenie czy reakcji (tylko raportowanie, blokowanie, kwarantanna)
    e. określenie reakcji w przypadku wykrycia nieznanych plików wykonywalnych: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie
    f. określenie listy zaufanych producentów oprogramowania
    g. określenie listy zaufanych procesów i folderów, z których można wykonywać pliki
    h. włączenie i wyłączenie wykrywania złośliwych makr w plikach pakietu Microsoft Office
    i. określenie reakcji w przypadku wykrycia nieznanych plików makr: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie
    j. określenie harmonogramu periodycznego automatycznego skanowania dysków z możliwością wykluczenia listy folderów
    k. włączenie/wyłączenie ochrony przed wykradaniem haseł
    l. włączenie/wyłączenie ochrony przed przekierowaniem standardowych strumieni wejścia i wyjścia na gniazdka sieciowe (tzw. network sockets)
    m. określenie reakcji w przypadku wykrycia nieznanych plików makr: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie
52. System musi posiadać możliwość dostrajanie działania poszczególnych silników inspekcji a w szczególności możliwość tworzenia wyjątków w ich funkcjonowaniu per nazwa procesu

53. System musi umożliwiać blokowanie uruchamiania plików z zewnętrznych nośników danych takich jak przenośna pamięć flash (usb pendrive) i napęd cd-rom
54. System musi umożliwiać zdalne odcięcie chronionego systemu od dostępu sieciowego z możliwością wskazania listy procesów, które zachowają dostęp do sieci
55. Agent musi posiadać opcję pobierania aktualizacji silników inspekcji od innych agentów w tej samej sieci, które już zostały zaktualizowane w celu oszczędzania pasma łącza Internetowego

I.6. CENTRALNY SYSTEM CHRONIONEGO, NADZOROWANEGO DOSTĘPU DO SIECI INTERNET ORAZ ZASOBÓW PUBLIKOWANYCH W INTERNECIE PRZEZ ZAMAWIAJĄCEGO

1. W zakresie tego elementu Zamawiający wymaga dostarczenia platformy sprzętowej, wykonanie wdrożenia oraz utrzymania centralnego dostępu do zasobów zgodnie z poniższą specyfikacją.
2. Zamawiający wymaga dostarczenia dwóch urządzeń bezpieczeństwa NGF Next-Generation Firewall na brzegach sieci Internet Zamawiającego, mogących działać jako klaster wysokiej dostępności lub jako dwa niezależne urządzenia.
3. Wymagane jest dostarczenie wsparcia producenta urządzeń na cały okres umowy (36 miesięcy). Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.
4. Zamawiający wymaga:
    a) bezpośredniej terminacji wewnętrznych sieci LAN na urządzeniach NGF,
    b) spięcia urządzeń NGF łączem Ethernet w celu zapewnienia ciągłości działania dostępu do sieci Internet. Połączenie to może być realizowane z wykorzystaniem łączy określonych w części: I.1. SIEĆ IP VPN MPLS. W przypadku niedostępności jednego z urządzeń NGF, Zamawiający oczekuje automatycznego przełączenia usługi działania dostępu do sieci Internet na drugie urządzenie.
    c) spięcia, a następnie uruchomienia routingu dynamicznego BGP pomiędzy urządzeniami NGF a routerami CE,
    d) dla punktów dostępowych: terminacji publicznej adresacji IP na urządzeniach NGF,
    e) dla punktów dostępowych: translacji NAT/PAT realizowana na urządzeniach NGF,
    f) dostępu do Internetu w oparciu o uwierzytelnianie oraz autoryzację na urządzeniach NGF w oparciu o serwer katalogowy AD Zamawiającego.
    g) wdrożenie niezbędnych polityk bezpieczeństwa (reguł) zgodnie z wytycznymi, które zostaną przekazane Wykonawcy na etapie wdrożenia systemu.
5. Dodatkowo Zamawiający wymaga zapewnienia na styku sieci WAN-LAN ochrony elektronicznych usług Zamawiającego udostępnianych do Internetu (www, poczta, dns, ftp itd.) przed zagrożeniami z sieci internetowej. Usługa powinna zawierać m.in. mechanizmy: flood protection, threat prevention. Zamawiający dopuszcza wykorzystanie urządzeń bezpieczeństwa NGF Next-Generation Firewall zlokalizowanych na brzegach sieci Internet w punktach dostępowych.
6. Centralny system bezpieczeństwa, który będzie zarządzany i utrzymywany przez Wykonawcę, ma umożliwić administratorom Zamawiającego:
    a) samodzielne zarządzanie regułami dostępu do i z sieci Internet,

b) przeglądanie zarejestrowanych zdarzeń sieciowych,
c) wykonywanie podstawowych czynności diagnostycznych (ping, tracert, kontrola stanu połączeń).

7. Wymagane jest, aby wszystkie czynności administracyjne wykonywane w systemie bezpieczeństwa przez administratorów Zamawiającego, jak również przez administratorów Wykonawcy, były rejestrowane oraz przechowywane przez czas trwania umowy.
8. Zamawiający oczekuje przeprowadzenia dwudniowego szkolenia z obsługi dostarczonego centralnego systemu bezpieczeństwa dla max. 3 osób ze strony Zamawiającego.
9. Zamawiający wymaga dostarczenia schematu umiejscowienia urządzeń bezpieczeństwa.
10. Szczegółowe wymagania w zakresie wymaganych dwóch urządzeń bezpieczeństwa określa poniższa tabela:

Nr	Wymagania minimalne
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta.
2	Urządzenie musi być wyposażone w ➢ 12 interfejsów 10/100/1000 (RJ45) ➢ 4 interfejsy 1GE SFP+ ➢ 4 interfejsy 1/10GE SFP+ obsadzone dwoma modułami 10GE SFP+ SR i dwoma modułami 10GE SFP+ LR. Zamawiający dopuszcza by urządzenie zamiennie dla czterech interfejsów 1/10GE było wyposażone w 4 (cztery) interfejsy 10GE i 4 (cztery) interfejsy 1GE; nie zmienia to wymagań względem pozostałych wymaganych interfejsów.
3	Urządzenie musi być wyposażone dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w moduł klasy Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania)
4	Urządzenie musi być wyposażone w dysk HDD lub SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 200GB
5	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 4,5 Gbps dla Firewall/kontroli aplikacji Minimum 2,2 Gbps dla Firewall/IPS/kontroli aplikacji/antymalware Minimum 50 tys. nowych połączeń na sekundę. Minimum 1.000.000 równoległych sesji Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Jako scenariusz Firewall/IPS/kontroli aplikacji/antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, antymalware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antymalware, ochrony DNS
6	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. rutera (tzn. w warstwie 3 modelu OSI), b. przełącznika (tzn. w warstwie 2 modelu OSI), c. w trybie pasywnego nasłuchu (sniffer).

7	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu
8	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
9	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
10	Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
11	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 2 Gbps dla IPSEC VPN Minimum 1 000 tuneli IPSEC VPN (site-to-site) Minimum 1 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (co najmniej dla Windows) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 1000 jednoczesnych użytkowników
12	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ➢ oznaczania pakietów znacznikami DiffServ, ➢ utworzenia co najmniej 8 klas ruchu sieciowego. ➢ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.
13	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
14	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
15	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
16	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
17	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 100 stref bezpieczeństwa.
18	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
19	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
20	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia
21	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji
22	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”
23	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.

24	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH
25	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services. d) logi z syslog
26	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
27	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia
29	Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Zamawiający wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia. Jeżeli producent rozwiązania dodatkowo licencjonuje liczbę plików przesyłanych automatycznie (przez urządzenie) do chmurowego sandboxa wówczas należy przyjąć wartość 5 000 plików dziennie
30	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia
31	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia
32	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet
33	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.

	Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia
34	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
35	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu: a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu b. Operator, który ma możliwość tylko odczytu konfiguracji. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ d. SAML 2,0 Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS
36	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Realizacja tego wymagania musi opierać się o samo urządzenie – nie dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Funkcja ta musi być dostępna również w przypadku utraty komunikacji z centralną konsolą zarządzania. Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI)
37	Urządzenie musi zapewniać interfejs API (JSON lub REST lub XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)
38	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.
39	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
40	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.
41	Urządzenie musi posiadać funkcjonalność sieciowego Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV nie może wprowadzać zmniejszenia wydajności urządzenia tzn. że przepustowość urządzenia z włączonymi wszystkimi modułami wykrywania ataków (w tym AV) nie może być mniejsza niż 2,3 Gb/s.
42	W ramach funkcjonalności ochrony przed atakami day 0 i współpracy z sandboxem system pozwala by administrator posiadał dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również zapewnia możliwość manualnego wysłania pliku (upload przez stronę www) do sandboxa. Jeżeli producent rozwiązania dodatkowo licencjonuje liczbę plików przesyłanych manualnie do chmurowego sandboxa wówczas należy przyjąć wartość 200 plików dziennie.
43	Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich.

44	Urządzenie Firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. Cykl/interwał odświeżania polityk bezpieczeństwa urządzenia firewall nie może być dłuższy niż 5 minut.

II. WYMAGANIA SZCZEGÓŁOWE ZWIĄZANE Z PRZEDMIOTEM ZAMÓWIENIA

1. Wykonawca musi posiadać lub dysponować siecią szkieletową.
2. Wykonawca zapewni w każdym czasie okresu realizacji przedmiotu zamówienia możliwość priorytetyzacji ruchu pakietów IP Zamawiającego na całym odcinku sieci (również w sieci Wykonawcy).
3. Wykonawca zdefiniuje w sieci VPN Zamawiającego 1 klasę usługową (CoS) dedykowane celom transmisji danych.
4. Zmawiający zastrzega sobie w każdym czasie trwania realizacji przedmiotu zamówienia zmianę ilości klas usługowych (CoS) bez dodatkowych kosztów.
5. Rozszerzenie klas ruchu przez Zamawiającego nie przekroczy 5 klas, w tym dedykowane klasy dla transmisji głosu i obrazu.
6. Procentowy podział pasma łącza dostępowego na klasy ruchu zostanie zdefiniowany przez Zamawiającego.
7. Odwzorowanie ruchu pakietów IP Zamawiającego na CoS sieci VPN musi opierać się o:
   a. znacznik DSCP
   b. znacznik IEEE 802.1p
   c. adresy IP/porty źródłowe/docelowe
8. Wykonawca zagwarantuje całodobowe, telefoniczne wsparcie techniczne przez cały okres świadczenia usługi.
9. Wykonawca zagwarantuje SLA o następujących parametrach:
   a. Godzinową, roczną dostępność placówki na poziomie co najmniej 99,6%
   b. Usunięcie awarii lub uszkodzenia placówki w przeciągu max. 8 godzin zagwarantowane przez cały okres świadczenia usługi. Usunięcie awarii lub usterki będzie poprzedzone powiadomieniem ze strony Wykonawcy dedykowanej osoby/osób ze strony Zamawiającego o podjętych działaniach naprawczych.
   c. W przypadku odwzorowania ruchu pakietów IP Zamawiającego na CoS sieci VPN Wykonawcy, Wykonawca będzie w stanie zagwarantować dla min. dwóch klas ruchu danych średnią (w cyklu dobowym) wartość parametru RTD na dobowym poziomie nie przekraczającym 75 ms. Dodatkowo Zamawiający oczekuje, iż przynajmniej jedna z klas ruchu danych Wykonawcy zagwarantuje średnią dobową wartość parametru LPR na poziomie nie przekraczającym 0,2%.
10. Na żądanie Zamawiającego, Wykonawca będzie zobowiązany do co najmniej jednej, bezpłatnej (w skali miesiąca) zmiany konfiguracji routerów we wskazanych placówkach. Zmiany konfiguracji routerów mogą dotyczyć m.in. rozszerzenia/zawężenia maski dla obsługiwanych podsieci Zamawiającego, zmiany wynikające z kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej (przez wykorzystanie reguł firewall, access-list, ustawianie routingu) itp.