Opis Przedmiotu Zamówienia na

dostawę urządzeń typu Next Generation Firewall

I. Wymagania ogólne

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek europejski.
2. Całość dostarczanego sprzętu musi być fabrycznie nowa (nie używana w innych środowiskach).
3. Urządzenia nie mogą być używane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
4. Całość dostarczanego sprzętu musi być dostępna w obecnej ofercie produktowej producenta oraz nie może być przeznaczona do wycofania z produkcji, sprzedaży bądź wsparcia (end-of-life, end-of-sale, end-of-support).
5. Wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje, jak też samo urządzenie musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta)
6. Sprzęt musi zostać dostarczony z najnowszą wersją oprogramowania systemowego (firmware) lub z wersją oprogramowania rekomendowaną przez producenta oferowanego rozwiązania. Jeżeli urządzenia są fabrycznie wysyłane z inną wersją oprogramowania to Wykonawca zobowiązany jest do dostarczenia wersji najnowszej lub wersji rekomendowanej przez producenta (na nośniku, poprzez wskazanie jej lokalizacji w portalu producenta z możliwością jej pobrania, lub też poprzez pobranie jej bezpośrednio na urządzenie itp.)
7. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, żeby była możliwa identyfikacja zarówno produktu jak i producenta.
8. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych producenta.
9. W przypadku wymiany nośników danych, które uległy awarii, uszkodzone nośniki muszą pozostać w całości u Zamawiającego. Nie przewiduje się opcji demontażu dysków i pozostawienia u Zamawiającego fragmentów dysków z nośnikami danych.
10. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej (dopuszczalne jest dostarczenie dokumentacji w języku angielskim).
11. Wszystkie urządzenia muszą posiadać Certyfikat CE produktu.
12. System musi być objęty minimum 12 miesięczną gwarancją przez centrum serwisowego w rygorze następny dzień roboczy. W ramach gwarancji, muszą być serwisowane wszystkie elementy sprzętu, zapewniony dostęp do baz wiedzy producenta, aktualizacji oprogramowania oraz nieograniczony dostęp do TAC (Technical Assistance Center). W ramach gwarancji muszą być również dostępne wszystkie licencje/subskrypcje na okres minimum 12 miesięcy zapewniające opisane wyżej funkcjonalności.

II. Wdrożenie

1. Zamawiający wymaga zapewnienia certyfikowanych inżynierów na czas wdrożenia. W ramach wdrożenia całość zostanie zintegrowana z siecią Zamawiającego.
2. W ramach wdrożenia, inżynierowie zainstalują zaoferowane urządzenia NGF w wyznaczonym przez Zamawiającego miejscu, podłączą do sieci zamawiającego oraz dostosują i przeniosą konfigurację z posiadanych przez Zamawiającego urządzeń NGF typu PaloAlto PA3020.
3. Inżynierowie muszą posiadać odpowiednią wiedzę i doświadczenie – minimum dwóch inżynierów z certyfikatami producenta[1] dostarczanego rozwiązania.
4. Inżynierowie muszą posiadać odpowiednią wiedzę i doświadczenie – minimum dwóch inżynierów z

[1] Opis warunków które musi spełnić certyfikat producenta zaoferowanego rozwiązania znajduje się w dokumencie „Warunki równoważności dotyczące znaków towarowych wskazanych w treści Umowy i załączników”

certyfikatem BCNP lub równoważnym[2] – osoby te będą odpowiedzialne za konfigurację przełączników Brocade posiadanych przez Zamawiającego.

5. Wszyscy inżynierowie muszą się biegle porozumiewać w języku polskim w mowie i piśmie.
6. Wykonawca w ramach wdrożenia przeszkoli trzech pracowników Zamawiającego z zaoferowanego rozwiązania

III. Centralny System zarządzania, logowania i raportowania urządzeniami bezpieczeństwa – maszyna wirtualna

1. System zarządzania musi obsługiwać minimum 25 urządzeń firewall.
2. W przypadku gdy Wykonawca zaoferuje rozwiązanie nie spełniające powyższych wymagań, Zamawiający dopuszcza, w ramach wynagrodzenia, wymianę posiadanych urządzeń na równoważne. Opis równoważności znajduje się w dokumencie „Warunki równoważności dotyczące znaków towarowych wskazanych w treści Umowy i załączników"
3. System zarządzania musi współpracować z pełni (wszystkie funkcje) z dostarczanym klastrem firewall w ramach tego postępowania.
4. System zarządzania musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 12 TB.
5. System zarządzania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie.
6. System zarządzania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
7. System zarządzania musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
8. System zarządzania musi umożliwiać przeszukiwanie skorelowanych logów zebranych z zarządzanych firewalli.
9. System zarządzania musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
10. System zarządzania musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
11. System zarządzania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down".
12. System zarządzania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) i globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).
13. System zarządzania musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).
14. System zarządzania musi umożliwiać tworzenie raportów na podstawie zbudowanych kontenerów.
15. System zarządzania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
16. System zarządzania musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.
17. System zarządzania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
18. System zarządzania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek.
19. System zarządzania musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli.
20. System zarządzania musi pozwalać na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu konsoli zarządzającej.
21. System zarządzania musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
22. System zarządzania musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne).
23. System zarządzania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
24. System zarządzania musi informować o zmianach konfiguracji systemu.

[2] Opis warunków równoważności znajduje się w dokumencie „Warunki równoważności dotyczące znaków towarowych wskazanych w treści Umowy i załączników"

25. System zarządzania musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem.
26. System zarządzania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.
27. System zarządzania musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał iż nowe urządzenie zastępuje urządzenie uszkodzone.
28. System zarządzania musi być dostarczony jako maszyna wirtualna, zgodna ze środowiskiem Hyper-V posiadanym przez Zamawiającego.
29. Wymagane jest dostarczenie licencji na okres 12 miesięcy na wszystkie wymienione w OPZ funkcjonalności systemu.

IV. System zarządzania musi współpracować z posiadanymi przez Zamawiającego urządzeniami firewall: PaloAlto Networks PA-220, co najmniej w poniższym zakresie:

a) możliwości zbierania logów poprzez protokół syslog;
b) zbierane dane muszą zawierać informacje co najmniej o:
- ruchu sieciowym,
- użytkownikach,
- aplikacjach,
- zagrożeniach,
- filtrowanych stronach WWW.

System zarządzania może również współpracować z posiadanymi przez Zamawiającego urządzeniami firewall: PaloAlto Networks PA-220 w pełnym zakresie opisanym w ramach kryterium oceny ofert.

V. Urządzenie typu Next Generation Firewall – Dwa urządzenia pracujące jako jeden klaster wysokiej dostępności (HA)

1. Urządzenia muszą być dostarczone jako dedykowane urządzenia typu appliance, przystosowane do montażu w szafie Rack 19”. Całość sprzętu musi być zarządzana przez jednego producenta.
2. Urządzenie musi być wyposażone w:
   a. minimum 12 interfejsów 1/10GE miedzianych (RJ45)
   b. minimum 10 interfejsów 1/10GE SFP+. Należy dostarczyć minimum 8 wkładek 10GE SR wraz z urządzeniem.
   c. minimum 4 interfejsy 25GE – wkładki SFP28. Należy dostarczyć minimum 2 wkładki 25GE SR wraz z urządzeniem.
3. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   Minimum 11.5 Gbps (ruch typu „appmix”) dla Firewall/kontroli aplikacji
   Minimum 5,7 Gbps (ruch typu „appmix”) dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware
   Minimum 144000 nowych połączeń (sesji) na sekundę
   Minimum 1400000 równoległych/jednoczesnych zestawionych 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/Antywirus/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, Antywirus, Anty Spyware. 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, antywirus i antyspyware.
4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe dla ruchu szyfrowanego (IPSEC VPN, SSL VPN):
   Minimum 6.5 Gbps dla IPSEC VPN
   Minimum 3000 tuneli IPSEC VPN (site-to-site)
   Minimum 1000 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.
5. Urządzenie musi posiadać dysk Flash SSD o pojemności minimum 450GB.

6. 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.
7. Urządzenie musi umożliwiać działanie w co najmniej 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).
8. 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 (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)
9. 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.
10. 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.
11. Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:
    a. oznaczania pakietów znacznikami DiffServ,
    b. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,
    c. utworzenia co najmniej 8 klas ruchu sieciowego,
    d. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
12. Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
13. Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
14. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.
15. Urządzenie musi obsługiwać wirtualne instancje firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 10 takich systemów za pomocą licencji. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
    a. Tablic routingu
    b. Polityk bezpieczeństwa obejmujących: System IPS, System ochrony antymalware/antyspyware, System ochrony antywirus
    c. Koncentratorów VPN dla zdalnego dostępu
16. Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
17. 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.
18. Urządzenie musi wspierać obsługę klastrowania dla kilku Data Center, gdzie urządzenia firewall umieszczone są w różnych Data Center (np. trzy ośrodki Data Center, gdzie w każdym mamy po dwa urządzenia). W ramach tej funkcji urządzenie musi się potrafić tworzyć klaster z minimum 6 urządzeń.
19. Urządzenie musi posiadać wspierać funkcjonalność Network Packet Broker, gdzie dany ruch może być wysłany dodatkowo do kolejnych urządzeń/narzędzi bezpieczeństwa takich jak systemy SIEM, IPS/IDS, nagrywarki ruchu.
20. 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 10000 reguł polityki bezpieczeństwa oraz obsługę minimum 200 stref bezpieczeństwa.
21. 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 65535 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.

22. Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
23. 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.
24. 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.
25. 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.
26. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download".
27. Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
28. Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
29. 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,
30. 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.
31. 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 wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.
32. Urządzenie musi posiadać funkcjonalność 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 musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia.
33. Urządzenie musi zapewniać ochronę przed atakami typu Spyware. Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub 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 być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana 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.
34. 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.

35. Funkcja ochrony DNS musi wykrywać ataki bazującym na tunelowaniu ruchu poprzez protokół DNS.
36. Urządzenie musi za pomocą sprawdzania DNS (np. w połączeniu z URL Filtering) wykonywać klasyfikację ryzyka otwieranych stron Web – wykrywać nowo zarejestrowane domeny, mieć widzę na temat domen związanych ze złośliwym działaniem, analizować zawartość stron phishing'owych.
37. Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
38. Urządzenie musi posiadać 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.
39. Urządzenie musi posiadać funkcjonalność ochrony przed atakami zero-day i współpracy z sandboxem. Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand Box" plików różnych typów co najmniej exe i dll, przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Zamawiający nie wymaga dostarczenia licencji w chwili zakupu urządzenia.
40. 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).
41. 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.
42. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą:
    a. bazy lokalnej,
    b. serwera LDAP,
    c. RADIUS lub TACACS+
    d. SAML 2,0
43. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
44. 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. Funkcja musi być dostępna co najmniej w interfejsie GUI.
45. Urządzenie musi zapewniać interfejs API (JSON, REST, 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).
46. Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
47. Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
48. Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
49. Urządzenie musi być wyposażone w redundantne zasilacze typu AC pracujące redundantnie.

50. Wymagane jest dostarczenie licencji na okres 12 miesięcy na wszystkie wymienione w OPZ funkcjonalności urządzeń.