*Załącznik nr 2B do SWZ nr DZP.381.102.2020.DW (zm.)*

**Opis przedmiotu zamówienia - CZĘŚĆ B**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **NAZWA URZĄDZENIA**  Parametry wymagane przez Zamawiającego | **Liczba sztuk** | **OPIS TECHNICZNY OFEROWANEGO URZĄDZENIA**  Należy wskazać wszystkie elementy składowe oferowanego urządzenia w odniesieniu do kolumny z lewej strony | **INDEX** |
| 1. | **Firewall**  Urządzenie winno być wyposażone w zasilanie redundantne (2 x AC).  Urządzenie winno umożliwić tworzenie wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Urządzenie winno umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia pracujące w klastrze muszą mieć możliwość funkcjonowania w trybach Active/Passive i Active/Active.  Dostarczone w ramach niniejszego postępowania urządzenia muszą umożliwić konfigurację taką, iż w przypadku awarii jednego z nich wznowienie ochrony nastąpi w czasie nie dłuższym niż 30 minut  Urządzenia winno być dostarczone jako dedykowane urządzenie typa appliance, przystosowane do montażu w szafie Rack 19” o maksymalnej wysokości 4U każde.  Urządzenie musi być wyposażone w co najmniej:   * + - 4 interfejsy 40GE QSFP+.     - 4 interfejsy 100/1000/10GE Ethernet (RJ45),     - 8 interfejsów 1/10GE SFP+ (obsadzone modułami 10GE SFP+ SR),     - 8 interfejsów 1GE SFP,   Dopuszczalne jest rozwiązanie realizujące 4 interfejsy 1000/10GE Ethernet (RJ45) w oparciu o wkładki SFP+ GC. W tej sytuacji urządzenie ma być wyposażone w co najmniej 12 interfejsów 1/10GE SFP+  Urządzenie winno być wyposażone dedykowany port konsoli/zarządzania. Port ten winien być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji,  Urządzenie winno spełniać co najmniej następujące parametry wydajnościowe przy czym jeżeli urządzenie może pracować w różnych trybach, to jego wydajność musi być mierzona w trybie pracy, który pozwala na uruchomienie wszystkich wymaganych funkcji urządzenia:   * + - minimum 16 Gbps dla Firewall/kontroli aplikacji,     - minimum 8 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji,     - minimum 100 tys. nowych połączeń na sekundę,     - minimum 4.000.000 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/Antywirus/kontroli aplikacji” 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, antyspyware, ochrony DNS.  Urządzenie winno umożliwiać działanie co najmniej w trzech trybach pracy   * + - rutera (tzn. w warstwie 3 modelu OSI),     - przełącznika (tzn. w warstwie 2 modelu OSI)     - w trybie pasywnego nasłuchu (sniffer).   Tryb pracy urządzenia winien 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.).  Urządzenie winno 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.  Urządzenie winno 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.  Urządzenie winno umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.  Konfiguracja VPN winna odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.  W kontekście VPN urządzenie winno spełniać co najmniej następujące parametry wydajnościowe:   * + - Minimum 10 Gbps dla IPSEC VPN,     - Minimum 5 000 tuneli IPSEC VPN (site-to-site)     - Minimum 5 000 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 (dla systemów: Windows, Linux, MacOS) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 5 000 jednoczesnych użytkowników.  Urządzenie winno umożliwić monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  Urządzenie winno umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach:   * + - polityki definiujące powinny umożliwiać wykorzystanie:       * adresów źródłowych,       * adresów docelowych,       * użytkowników,       * numerów portów usług ,       * kategorii URL,     - system winien obsługiwać co najmniej następujące mechanizmy uwierzytelnienia       * RADIUS lub TACACS+,       * LDAP,       * Kerberos lub SAML 2.0.   Urządzenie winno zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:   * + - oznaczania pakietów znacznikami DiffServ,     - ustawiania dla dowolnych aplikacji oraz wybranych kategorii url: priorytetu, pasma maksymalnego i gwarantowanego,     - utworzenia co najmniej 8 klas ruchu sieciowego,     - kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.   Urządzenie winno posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.  Urządzenie winno umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.  Urządzenie winno posiadać funkcjonalność definiowania co najmniej 10 wirtualnych firewalli z możliwością rozbudowy w przyszłości do co najmniej 20 wirtualnych firewalli umożliwiających konfigurowanie dla każdego z nich indywidualnie i niezależnie od innych wirtualnych firewalli:   * + - tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych),     - polityk bezpieczeństwa obejmujących: system IPS, system ochrony antymalware/antyspyware, system ochrony antywirusowej,     - koncentratorów VPN dla zdalnego dostępu.   Dopuszczalne jest, aby zaoferowane urządzenie nie oferowało możliwości uruchomienia więcej niż jednego wirtualnego routera per wirtualny firewall. W tej sytuacji zaoferowana konfiguracja musi mieć możliwość konfiguracji 20 wirtualnych firewalli z możliwością rozbudowy do 40 wirtualnych firewalli.  Polityka bezpieczeństwa systemu zabezpieczeń winna 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. Zarządzanie pasmem QoS może odbywać z poziomu polityki bezpieczeństwa lub też z poziomu osobnych, dedykowanych polityk dotyczących zarządzania pasmem.  Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 1000 stref bezpieczeństwa.  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 2000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.  Urządzenie winno i przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa.  Urządzenie winno pozwalać na blokowanie transmisji plików co najmniej następujących typów: 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.  Urządzenie winno zapewniać ochronę przed atakami typu „Drive-by-download”.  Urządzenie winno posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.  Urządzenie winno zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.  Rozwiązanie winno umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:   * + - Microsoft Active Directory,     - usługi katalogowe LDAP,     - serwery Terminal Services,     - informacje z logów SYSLOG,   przy czym dopuszczalne opuszcza możliwość zastosowania zewnętrznego systemu uwierzytelnienia, przy założeniu, iż będzie on dostarczony w postaci dedykowanego urządzenia tego samego producenta co oferowany Firewall i pozwalającego na obsługę minimum 5000 użytkowników.  Polityka kontroli dostępu urządzenia winna 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.   * + - Urządzenie winno posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. Zamawiający wymaga spełnienia następujących wymagań:     - System IPS/IDS winien działać w warstwie 7 modelu OSI.     - Baza sygnatur IPS/IDS winna być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny.     - Moduł IPS/IDS winien 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 winno zapewniać możliwość ręcznego tworzenia sygnatur IPS/IDS bezpośrednio na urządzeniu lub na poziomie centralnej konsoli zarządzania.     - Zamawiający wymaga dostarczenia licencji na IPS/IDS w momencie dostawy urządzenia.   Urządzenie winno posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Zamawiający wymaga spełnienia następujących wymagań:   * + - Moduł AV winien być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb.     - Baza sygnatur AV winna być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny.     - Moduł AV winien uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).   Urządzenie winno 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. Zamawiający wymaga spełnienia następujących wymagań:   * + - Baza sygnatur anty-spyware winna być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny.     - Reguły/silnik anty-spyware winien być 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 winno 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).  Urządzenie winno posiadać funkcję wykrywania aktywności sieci typu Botnet.  Urządzenie winno posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. Zamawiający wymaga spełnienia następujących warunktów:   * + - Baza web filtering winna być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 40 milionów rekordów URL.     - Moduł filtrowania stron WWW winien 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 winien zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bezpośrednio na urządzeniu lub z wykorzystaniem centralnej konsoli zarządzania.     - Zamawiający wymaga dostarczenia licencji do funkcjonalności URL Filtering.   Zamawiający wymaga spełnienia następujących wymagań w kontekście funkcjonalności sandbox:   * + - Urządzenie winno posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.     - Urządzenie winno umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Urządzenie musi umożliwić włączenie/wyłączenie funkcjonalności przesyłania do zewnętrznych systemów typu “Sand-Box".     - Zamawiający wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia.   Zarządzanie urządzeniem winno odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW.  Dostęp do urządzenia i zarządzanie z sieci winny być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).  System zabezpieczeń winien pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach .  Urządzenie winno umożliwiać uwierzytelnianie administratorów za pomocą:   * + - bazy lokalnej,     - serwera LDAP,     - RADIUS.   Urządzenie winno 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).  Urządzenie winno zapewniać możliwość zapisania min. 10 poprzednich wersji konfiguracji.  Praca na urządzeniu winna 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. Wymaganie zostanie uznane za spełnione jeśli taki tryb pracy jest możliwy z poziomu konsoli lub interfejsu graficznego urządzenia lub systemu do zarządzania zaporą sieciową.  Urządzenie winno 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.  Urządzenie winno umożliwiać bieżące wysyłanie logów do zewnętrznych serwerów SYSLOG.  Zarządzanie zaporą sieciową oraz system logowania i raportowania  Wraz z urządzeniami firewall konieczne jest dostarczenie centralnego systemu zarządzania, logowania i raportowania jako systemu realizującego funkcje zbierania logów, zarządzania uprawnieniami administratorów i inwentury, a także generowania raportów.  System zarządzania, logowania i raportowania winien zostać dostarczony w postaci urządzenia lub w postaci maszyny wirtualnej instalowanej w środowisku VMWare.  Dopuszczalne jest, aby system zarządzania, logowania i raportowania składał się z dwóch niezależnych komponentów, współpracujących ze sobą i pochodzących od jednego producenta, przy czym obydwa komponenty mogą być urządzeniami fizycznymi, obydwa mogą być maszynami wirtualnymi, jeden z komponentów może być urządzeniem fizycznym a drugi maszyną wirtualną. Rozwiązanie systemu zarządzania, logowania i raportowania zaoferowane w postaci dwu komponentów musi posiadać możliwości i funkcjonalność oraz zachowywać się tak jakby stanowiło jedno urządzenie.  System zarządzania, logowania i raportowania winien spełnić następujące wymagania minimalne:   * + - obsługa nie mniej niż 10 firewalli fizycznych,     - obsługa nie mniej niż 100 firewalli wirtualnych (Zamawiający wymaga dostarczenia licencji na tyle firewalli wirtualnych ile zostało przez niego zaoferowanych. Rozwiązanie musi być w stanie obsłużyć co najmniej 100 firewalli wirtualnych w przypadku doposażenia w odpowiednie licencje),     - obsługa co najmniej 10000 zdarzeń na sekundę,     - obsługa przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB. W przypadku zaoferowania rozwiązania sprzętowego przestrzeń urządzenia musi być zrealizowana w RAID-1 lub RAID-6 oraz posiadać użyteczną (po zabezpieczeniu) pojemność co najmniej 10TB.   System zarządzania, logowania i raportowania winien umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW  System winien umożliwiać korelację logów zdarzeń z zarządzanych firewalli,  System zarządzania, logowania i raportowania winien zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej:   * + - umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych,     - tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego.     - zapisywanie 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,   System zarządzania, logowania i raportowania winien umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej:   * + - budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu lokalnym (dla wybranych firewalli lub logicznych systemów firewalla), globalnym (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).     - umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów),     - Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń,     - umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium,     - umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych,     - umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi   System zarządzania, logowania i raportowania winien:   * + - umożliwiać dystrybucję i zdalną instalację nowych wersji systemu,     - umożliwiać tworzenie kopii zapasowych zarządzanych firewalli,     - umożliwiać dystrybucję i zdalną instalację nowych sygnatur,     - umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia / logicznego systemu przed jej zatwierdzeniem,     - pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli / logicznych systemów,     - umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone,     - informować o zmianach konfiguracji systemu.   System zarządzania, logowania i raportowania winien umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. | **2** |  |  |