####  **Załącznik nr 6 SWZ/ nr 1 do umowy**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wykaz oferowanego sprzętu wraz ze wskazaniem** w tym wykazie oznaczeń identyfikujących oferowany przedmiot zamówienia *(należy podać oferowane parametry – pod rygorem odrzucenia oferty);*

# Wymagania ogólne

# W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta.

# System bezpieczeństwa (UTM) – 2 sztuki

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie usług dostarczanych od dostawcy łącza internetowego.

|  |  |
| --- | --- |
| **Wymagania minimalne** | **Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.)** |
| Należy podać producenta i oferowany model |  |
| System realizujący funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |  |
| System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. |  |
| System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego
 |  |
| Redundancja, monitoring i wykrywanie awarii |
| W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewnić funkcję synchronizacji sesji. |  |
| System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |  |
| System musi umożliwić monitoring stanu realizowanych połączeń VPN. |  |
| System musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| Interfejsy, Dysk, Zasilanie |
| 1. System musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
* 10 portów Gigabit Ethernet RJ-45.
 |  |
| System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 4G/5G oraz instalacji oprogramowania z klucza USB. |  |
| System realizujący funkcję firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności 128 GB. |  |
| System musi umożliwić skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| System musi być wyposażony w zasilanie AC wraz z zasilaczem. |  |
| Parametry wydajnościowe |
| W zakresie Firewall’a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. |  |
| Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. |  |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. |  |
| Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. |  |
| Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - 1.3 Gbps. |  |
| Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - 650 Mbps. |  |
| Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – 600 Mbps. |  |
| Funkcje Systemu Bezpieczeństwa |
| W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje: |
| Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |  |
| Kontrola Aplikacji. |  |
| Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |  |
| Ochrona przed malware. |  |
| Ochrona przed atakami - Intrusion Prevention System. |  |
| Kontrola dostępu do stron WWW. |  |
| Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. |  |
| Zarządzanie pasmem (QoS, Traffic shaping). |  |
| Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |  |
| Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN. |  |
| Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. |  |
| Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. |  |
| Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |  |
| Polityki, Firewall |
| W ramach polityk i firewalla muszą być realizowane wszystkie poniższe funkcje: |
| Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |  |
| System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
 |  |
| W ramach systemu możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  |
| System wykorzystuje w politykach bezpieczeństwa zewnętrzne repozytoria zawierających: kategorie URL, adresy IP. |  |
| Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. |  |
| System posiada możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. |  |
| 1. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
 |  |
| Połączenia VPN |
| 1. W ramach połączeń VPN muszą być realizowane wszystkie poniższe funkcje:
 |
| 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewnić:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
 |  |
| 1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewnić:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
 |  |
| Routing i obsługa łączy WAN |
| W zakresie routingu rozwiązanie musi zapewnić obsługę: |
| Routingu statycznego. |  |
| Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). |  |
| Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. |  |
| Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. |  |
| ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. |  |
| BFD (Bidirectional Forwarding Detection). |  |
| Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |  |
| Funkcje SD-WAN |
| System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. |  |
| SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |  |
| Zarządzanie pasmem |
| System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |  |
| System daje możliwość określania pasma dla poszczególnych aplikacji. |  |
| System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. |  |
| System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| Ochrona przed malware |
| W ramach systemu ochrony przez malware muszą być realizowane wszystkie poniższe funkcje: |
| Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |  |
| Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. |  |
| System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. |  |
| System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. |  |
| System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego). |  |
| Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. |  |
| System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. |  |
| Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |  |
| Ochrona przed atakami |
| W ramach systemu ochrony przed atakami muszą być realizowane wszystkie poniższe funkcje: |
| Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |  |
| System chroni przed atakami na aplikacje pracujące na niestandardowych portach. |  |
| Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. |  |
| System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |  |
| System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.  |  |
| Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). |  |
| Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. |  |
| Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |  |
| Kontrola aplikacji |
| W ramach kontroli aplikacji muszą być realizowane wszystkie poniższe funkcje: |
| Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |  |
| Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |  |
| Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  |  |
| Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |  |
| Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). |  |
| System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |  |
| Kontrola WWW |
| W ramach kontroli WWW muszą być realizowane wszystkie poniższe funkcje: |
| Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |  |
| W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. |  |
| Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. |  |
| Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |  |
| Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). |  |
| Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. |  |
| Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. |  |
| Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. |  |
| System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |
| Uwierzytelnianie użytkowników w ramach sesji |
| W ramach uwierzytelnianie użytkowników w ramach sesji muszą być realizowane poniższe funkcje: |
| System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. |  |
| System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. |  |
| System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. |  |
| Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |  |
| Zarządzanie |
| W ramach systemu zarządzania muszą być realizowane wszystkie poniższe funkcje: |
| Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. |  |
| Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |  |
| System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. |  |
| System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |  |
| Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |  |
| Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). |  |
| Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |  |
| Logowanie |
| W ramach systemu logowania muszą być realizowane wszystkie poniższe funkcje: |
| Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |  |
| W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |  |
| Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. |  |
| Możliwość włączenia / wyłączenia logowania per reguła w polityce firewall. |  |
| System zapewnia możliwość logowania do serwera SYSLOG. |  |
| Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |  |
| Testy wydajnościowe oraz funkcjonalne |
| Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy wydajnościowe. |  |
| Serwisy i licencje |
| Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy. |  |
| Gwarancja oraz wsparcie |
| Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |
| Rozszerzone wsparcie serwisowe AHB/SOS |
| System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres co najmniej 60 miesięcy.Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001:2015 lub równoważny w zakresie świadczenia usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Wymagania powinny być potwierdzone dokumentem oświadczanie wykonawcy lub producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) dołączyć do oferty. |  |

# Wymagania ogólne

# W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta (z wyłączeniem serwera do instalacji oprogramowania). Zamawiający aktualnie dysponuje 20 urządzeniami Fortigate-60F i oferowany systemu musi umożliwiać pełną współpracę oraz pełną integrację, ze wskazanymi urządzeniami.

# System centralnego logowania – 1 sztuk

|  |  |
| --- | --- |
| Wymagania minimalne | Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.) |
| A. System centralnego logowania |
| Wymagania ogólne |
| Należy podać producenta i model oferowanego rozwiązania |  |
| W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń |  |
| Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: Microsoft Hyper-V Server 2010, 2012 R2, 2016, 2022; VMware ESXi, ESX wersje:4,5,6; Xen, Microsoft Azure. |  |
| Interfejsy, Dysk |
| System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB. |  |
| Parametry wydajnościowe |
| System musi być w stanie przyjmować minimum 10 GB logów na dzień. |  |
| Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |  |
| Logowanie |
| Podgląd logowanych zdarzeń w czasie rzeczywistym. |  |
| Możliwość przeglądania logów historycznych z funkcją filtrowania.  |  |
| System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:* Listę najczęściej wykrywanych ataków.
* Listę najbardziej aktywnych użytkowników.
* Listę najczęściej wykorzystywanych aplikacji.
* Listę najczęściej odwiedzanych stron www.
* Listę krajów, do których nawiązywane są połączenia.
* Listę najczęściej wykorzystywanych polityk Firewall.
* Informacje o realizowanych połączeniach IPSec.
 |  |
| Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. |  |
| Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. |  |
| System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| Raportowanie |
| W zakresie raportowania system musi zapewniać: |
| Generowanie raportów co najmniej w formatach: PDF, CSV. |  |
| Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. |  |
| Funkcję definiowania własnych raportów.  |  |
| Możliwość spolszczenia raportów. |  |
| Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| Korelacja logów |
| W zakresie korelacji zdarzeń system musi zapewniać: |
| Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |  |
| Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |  |
| Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
 |  |
| Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.  |  |
| Zarządzanie |
| W zakresie zarządzania system musi zapewniać: |
| System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.  |  |
| Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. |  |
| System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
| Serwisy i licencje |
| Wsparcie: System musi być objęty serwisem producenta przez okres co najmniej 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
| B. System uwierzytelniania, autoryzacji i kontroli dostępu |
| Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje. |  |
| Należy podać producenta i model oferowanego rozwiązania |  |
| Parametry systemu |
| Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę:* 4 wirtualnych interfejsów sieciowych.

Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2, 2016, 2022; VMware ESXi, ESX wersje:4,5,6; Xen, Microsoft Azure. |  |
| **Parametry wydajnościowe i licencyjne** |
| System musi obsługiwać co najmniej:* Uwierzytelnianie dla 100 użytkowników.
* 25 tokenów dla uwierzytelniania dwuskładnikowego.
* 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu).
* Możliwość zdefiniowania co najmniej 10 grup użytkowników,
* 5 lokalnych centrów certyfikacji (CA).
* Możliwość wygenerowania 100 certyfikatów dla użytkowników.
 |  |
| **Wymagania ogólne** |
| System musi zapewniać nie mniej niż: |
| Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. |  |
| Graficzną reprezentację statusu uwierzytelnionych użytkowników. |  |
| 1. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:
* Lokalnie.
* Zdalnie w oparciu o protokół Syslog.
 |  |
| * Konfigurację Captive Portalu.
 |  |
| **Wymagania funkcjonalne – uwierzytelnianie** |
| Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: |
| * Lokalną, wbudowaną bazę użytkowników.
 |  |
| Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. |  |
| Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. |  |
| Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. |  |
| Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:* poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),
* czasu ważności hasła,
 |  |
| Konfigurowalną politykę blokowania kont, która będzie uwzględniać:* ilość nieudanych logowań,
* czas blokowania konta,
* okres nieaktywności, po którym konto jest blokowane.
 |  |
| Możliwość odzyskiwania haseł:* z wykorzystaniem adresu email,
* z wykorzystaniem pytania pomocniczego.
 |  |
| Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:* wbudowany serwer RADIUS,
* integrację z zewnętrznymi serwerami RADIUS – praca jako klient.
 |  |
| Obsługę protokołu LDAP, w tym zakresie system musi oferować:* wbudowany serwer LDAP,
* możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).
 |  |
| Obsługę protokołu SAML - Identity Provider (IdP) proxy. |  |
| Realizację funkcji SSO (Single Sign On) w oparciu o:* integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,
* dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,
* kontekst użytkownika przesyłany z serwera RADIUS,
* informacje uzyskiwane poprzez protokół Syslog.
 |  |
| **Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe** |
| Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż: |
| Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN. |  |
| Zamawiający dysponuje komputerami z zainstalowanym systemem Microsoft Windows 10 / 11 w wersji PRO. Należy zapewnić możliwość integracji z logowaniem do systemu Windows. |  |
| **Wymagania funkcjonalne – 802.1x** |
| System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: |
| Obsługa co najmniej poniższych protokołów EAP:* PEAP,
* EAP-TTLS,
* EAP-TLS,
* EAP-GTC.
 |  |
| Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication). |  |
| Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS. |  |
| **Wymagania funkcjonalne – zarządzanie certyfikatami** |
| System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: |
| Obsługa wbudowanego CA (Certificate Authority). |  |
| Obsługa CA pośredniczących (Intermediate CA). |  |
| Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. |  |
| Możliwość pobrania wygenerowanych certyfikatów. |  |
| Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. |  |
| Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. |  |
| Możliwość generowania certyfikatów typu wildcard. |  |
| Realizacja CRL (Certificate Revocation List). |  |
| Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). |  |
| Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| **Zarządzanie** |
| W zakresie zarządzania system musi zapewniać: |
| Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. |  |
| System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. |  |
| Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć. |  |
| Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| **Serwis** |
| Wymaga się aby dostawa obejmowała również serwis producenta przez okres co najmniej 60 miesięcy, uprawniający do aktualizacji oprogramowania oraz wsparcia technicznego w języku polskim w trybie 24x7. |  |
| C. Serwer do instalacji systemu centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu |
| Należy podać producenta i model oferowanego rozwiązania |  |
| Obudowa |
| Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android w wersji 11 – będący na wyposażeniu zamawiającego) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| Płyta główna |
| Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 56 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| Chipset |
| Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| Procesor |
| Zainstalowane dwa procesory każdy min. 12-rdzeniowy, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 216 w teście SPECrate2017\_int\_base, dostępnym na stronie [www.spec.org](http://www.spec.org) dla konfiguracji dwuprocesorowej. |  |
| RAM |
| Minimum 128GB DDR5 RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM. |  |
| Funkcjonalność pamięci RAM |
| Advanced ECC, Self Healing, Memory Health Check, DIMM Map Out, Memory Page Retire, Fault Resilient Memory |  |
| Gniazda PCI |
| Minimum trzy sloty PCIe x16 (2 gniazda 5 generacji 4, 1 gniazdo 4 generacji) możliwość zmiany slotów na min. 2 sloty PCIe x16 5 generacji |  |
| Interfejsy sieciowe/FC/SAS |
| Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)W komplecie dostarczone 2 wkładki SFP+ producenta serweraDodatkowa dwuportowa karta 32Gb FC. |  |
| Dyski twarde |
| Możliwość instalacji dysków SAS, SATA, SSDZainstalowane 5 dysków 1.92TB SSD vSAS Mixed Use 12Gbps 512e 2.5in Hot-Plug ,AG Drive SED, 3DWPD |  |
| Kontroler RAID |
| Sprzętowy kontroler dyskowy, posiadający min. 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. Wsparcie dla dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS. Gen3 (8 GT/s) and Gen4 (16 GT/s) NVMe |  |
| System operacyjny/System wirtualizacji |
| Microsoft Windows Serwer Standard 2022 2 core z ubezpieczeniem wersji na okres 3 lat w licencjonowaniu Microsoft MPSA – 24 sztukilub równoważny spełniający min. poniższe wymagania: * Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
* Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
* Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
* Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
* Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
* Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
* Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
* Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
* Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
* Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
* Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
* Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
* Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
* Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
* Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
* Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
* Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
* Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
* Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
* Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
* Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2019/2016.
 |  |
| Wbudowane porty |
| 4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA |  |
| Video |
| Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| Zasilacze |
| Redundantne, Hot-Plug min. 1400W każdy. |  |
| Bezpieczeństwo |
| * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
* Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Dane muszą być usunięte zgodnie ze standardem Instant Secure Erase.
* BIOS musi posiadać możliwość przełączenia do trybu uniemożliwiającego zmianę jego konfiguracji oraz jakiekolwiek zmianę w firmware komponentów serwera.
* Możliwość automatycznego przywrócenia BIOS do poprzedniej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.
 |  |
| Diagnostyka |
| Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| Karta Zarządzania |
| Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera bez konieczności instalacji dodatkowego oprogramowanie oraz niezależnie od zainstalowanego systemu operacyjnego
* Obsługa Redfish SSE
* Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android w wersji 11 – będący na wyposażeniu zamawiającego) przy użyciu jednego z protokołów BLE lub WIFI.
 |  |
| Oprogramowanie do zarządzania |
| * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
* integracja z Active Directory
* Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
* Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
* Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
* Szczegółowy opis wykrytych systemów oraz ich komponentów
* Możliwość eksportu raportu do CSV, HTML, XLS, PDF
* Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.
* Grupowanie urządzeń w oparciu o kryteria użytkownika
* Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
* Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
* Szybki podgląd stanu środowiska
* Podsumowanie stanu dla każdego urządzenia
* Szczegółowy status urządzenia/elementu/komponentu
* Generowanie alertów przy zmianie stanu urządzenia.
* Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
* Integracja z service desk producenta dostarczonej platformy sprzętowej
* Możliwość przejęcia zdalnego pulpitu
* Możliwość podmontowania wirtualnego napędu
* Kreator umożliwiający dostosowanie akcji dla wybranych alertów
* Możliwość importu plików MIB
* Przesyłanie alertów „as-is” do innych konsol firm trzecich
* Możliwość definiowania ról administratorów
* Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
* Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
* Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
* Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
* Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
* Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
* Zdalne uruchamianie diagnostyki serwera.
* Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
* Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
* Dostarczone oprogramowanie powinno umożliwiać stworzenie niestandardowego automatycznego działania dla wykrytego zdarzenia
* Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
* Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
* Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
* Integracja oprogramowanie zarządzającego z konsolami zarządzania typu vCenter i MS System Center
* Dostarczone oprogramowanie powinno umożliwiać zarządzanie urządzeniami firm trzecich bez potrzeby instalacji dedykowanego oprogramowania.
* Umożliwia aktualizację firmware i sterowników komponentów serwera
* Obsługa do minimum 8000 urządzeń per instancja
 |  |
| Certyfikaty |
| Serwer musi być wyprodukowany zgodnie z normami ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi. Serwer musi posiadać deklarację zgodności CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca dołączy do oferty dokument potwierdzający spełnianie wymogu.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.Zaoferowane w urządzeniu zasilacze muszą posiadać wydajność na poziomie Titanium. Do Oferty należy dostarczyć wydruk ze strony 80plus.org potwierdzający spełnienie wymogu.Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A, zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 lub równoważną dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - Wykonawca złoży dokument potwierdzający spełnianie wymogu. |  |
| Dokumentacja użytkownika |
| Zamawiający wymaga dokumentacji w języku polskim lub angielskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| Gwarancja oraz wsparcie |
| 60 miesięcy gwarancji producenta.Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem dedykowanej do tego celu aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik Wykonawcy lub Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia lub zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego do wyznaczonego Kierownika Eskalacji po stronie Wykonawcy.Zamawiający wymaga pojedynczego punktu kontaktu dla całego zaoferowanego rozwiązania, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających co najmniej: wykrywanie usterek sprzętowych z predykcją awarii oraz automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.Zamawiający wymaga od producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.Możliwość rozszerzenia gwarancji u Producenta zaoferowanego rozwiązania do co najmniej 84 miesięcy.Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący musi posiadać ISO 9001:2015 lub równoważny oraz ISO-27001 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzację producenta zaoferowanych urządzeń do wykonywania napraw – dokumenty potwierdzające należy załączyć do oferty.Wymagane dołączenie do oferty oświadczenia Wykonawcy lub Producenta potwierdzające, że serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta za pośrednictwem wykonawcy. |  |

# System centralnego zarządzania urządzeniami bezpieczeństwa oraz logowania – 1 sztuka

W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego Fortigate 60-F będącym na wyposażeniu zamawiającego. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej.

|  |  |
| --- | --- |
| Wymagania minimalne | Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.) |
| Należy podać producenta i oferowany model |  |
| Interfejsy, Dyski |
| System musi dysponować co najmniej:* 4 portami Gigabit Ethernet RJ-45,
* oraz portem konsoli szeregowej.
 |  |
| Powierzchnia dyskowa min. 8 TB. |  |
| Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1 |  |
| System musi być wyposażony w zasilanie AC. |  |
| Parametry wydajnościowe |
| System musi umożliwiać zarządzenie co najmniej 40 systemami bezpieczeństwa Fortigate 60-F lub wyższymi. |  |
| Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 40 systemów Fortigate 60-F lub wyższymi. |  |
| System musi być w stanie przyjmować minimum 2 GB logów na dzień. |  |
| Funkcje systemu centralnego zarządzania |
| W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje: |
| System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji). |  |
| System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi. |  |
| System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian). |  |
| System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej. |  |
| System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości. |  |
| System musi umożliwiać zarządzenie wersjami firmware’u oraz zapewniać centralną aktualizację oprogramowania. |  |
| System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń. |  |
| System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia). |  |
| System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami. |  |
| System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach. |  |
| System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM). |  |
| System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash. |  |
| Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |  |
| Funkcje logowania |
| Podgląd logowanych zdarzeń w czasie rzeczywistym. |  |
| Możliwość przeglądania logów historycznych z funkcją filtrowania.  |  |
| 1. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* Listę najczęściej wykrywanych ataków.
* Listę najbardziej aktywnych użytkowników.
* Listę najczęściej wykorzystywanych aplikacji.
* Listę najczęściej odwiedzanych stron www.
* Listę krajów, do których nawiązywane są połączenia.
* Listę najczęściej wykorzystywanych polityk Firewall.
* Informacje o realizowanych połączeniach IPSec.
 |  |
| Funkcja raportowania |
| Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. |  |
| Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. |  |
| Funkcję definiowania własnych raportów.  |  |
| Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| Funkcje korelacji |
| W zakresie korelacji zdarzeń system musi zapewniać: |
| Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |  |
| Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |  |
| Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
 |  |
| Zarządzanie |
| System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.  |  |
| Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI. |  |
| System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów. |  |
| System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API. |  |
| Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| Gwarancja oraz wsparcie |
| Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |  |

# Szkolenia, instalacja i konfiguracja

Należy wykonać szkolenie dla 25 pracowników Państwowej Inspekcji Sanitarnej z województwa zachodniopomorskiego (wskazanych przez zamawiającego) z obsługi urządzeń Fortigate 60F wyposażonymi w system operacyjny FortiOS w wersji 7.4.1. Szkolenie musi być przeprowadzone przez osobę / osoby legitymujące się certyfikatem na poziomie NSE8 (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta dostępnej (na dzień publikacji ogłoszenia) pod adresem: https://training.fortinet.com/mod/customcert/verify\_certificate.php). Szkolenie może obywać się zdalnie w grupach maksymalnie 10 osobowych. Długość szkolenia dla każdej grupy wynosi 3 dni robocze. Szkolenie musi być realizowane w języku polskim. Szkolenie musi zostać realizowane w ciągu 3 miesięcy od daty dostawy a termin szkolenia zostanie ustalony w porozumieniu z Wykonawcą.

W ramach dostawy należy wykonać także szkolenie dla 5 pracowników Państwowej Inspekcji Sanitarnej z województwa zachodniopomorskiego (wskazanych przez zamawiającego) z oferowanej technologii systemu centralnego zarządzania, systemów centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu. Szkolenie musi być przeprowadzone przez certyfikowanego w zakresie cyberbezpieczeństwa inżyniera oferowanej technologii. Poziom certyfikacji musi być na najwyższym poziomie dostępnym u producenta oferowanej technologii (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta zaproponowanego rozwiązania). Szkolenie może odbyć się zdalnie. Długość szkolenia wynosi 3 dni robocze. Szkolenie musi być realizowane w języku polskim. Szkolenie musi zostać realizowane w ciągu 3 miesięcy od daty dostawy a termin szkolenia zostanie ustalony w porozumieniu z Wykonawcą.

Wykonawca musi zapewnić wsparcie wdrożeniowe obejmujące całość zamówienia dla zamawiającego w wymiarze 80 godzin roboczych. Wsparcie musi być udzielone przez minimum dwóch inżynierów posiadających certyfikaty oferowanej technologii. Poziom certyfikacji musi być na najwyższym poziomie dostępnym u producenta oferowanej technologii (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta zaproponowanego rozwiązania). W przypadku gdy wsparcie zostanie udzielone przez producenta zaproponowanego rozwiązania a wsparcie będzie realizowane przez dużą grupę pracowników certyfikaty nie są wymagane. Całość procesu wsparcia musi być realizowana w języku polskim. Do kontaktu z inżynierami wyznaczeni zostaną pracownicy Państwowej Inspekcji Sanitarnej wskazani przez zamawiającego.