Załącznik nr. 4

Szczegółowy opis przedmiotu zamówienia

Zakup zintegrowanych sprzętowych zapór sieciowych / routerów UTM oraz kolektora/analizatora danych sieciowych (VM) na potrzeby zabezpieczenia infrastruktury teleinformatycznej Dolnośląskiej Instytucji Pośredniczącej.

Kody CPV:
Kod: 32413100-2
Opis: Rutery sieciowe
Kod: 48219100-7
Opis: Pakiety oprogramowania bramowego
Kod: 48219500-1
Opis: Pakiety oprogramowania do switcha lub routera
Kod: 48219000-6
Opis: Pakiety oprogramowania do różnych operacji sieciowych

Wymagania ogólne:

1. Dla jednoznacznej identyfikacji oferowanych rozwiązań należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego produktu lub jego oznaczenie kodowe wg. producenta. Zamawiający wymaga określenia oferowanych produktów i faktycznych parametrów, o których mowa w powyższym opisie, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany rozwiązanie spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane rozwiązania spełniają wymagania Zamawiającego. Ciężar wykazania spełnienia przez oferowane rozwiązania wymogów określonych przez Zamawiającego w specyfikacji spoczywa na składającym ofertę
2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
3. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
   W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
4. Pod pojęciem rozwiązań równoważnych, o ile nie dokonano doprecyzowania w danym zakresie, Zamawiający rozumie taki sprzęt i oprogramowanie, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w Opisie Przedmiotu Zamówienia.
5. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.
   Ciężar udowodnienia równoważności w stosunku do wymogów określonych przez Zamawiającego spoczywa na składającym ofertę. W takim przypadku Wykonawca musi przedłożyć odpowiednie dokumenty, opisujące parametry techniczne, wymagane prawem certyfikaty i inne dokumenty, dopuszczające dane produkty do użytkowania oraz pozwalające jednoznacznie określić, że są równoważne.
6. Dostarczane rozwiązanie musi być fabrycznie nowe i wcześniej nie wykorzystywane (odnosi się to zarówno do sprzętu jak i licencji oprogramowania).
7. Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
8. Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności licencjami na używanie tych funkcjonalności.
9. Wykonawca na potwierdzenie spełnienia wymagań i zapewnienia odpowiedniego poziomu świadczonych usług dołączy do oferty:
   - Oświadczanie, Producenta lub Autoryzowanego Dystrybutora na terytorium Polski świadczącego wsparcie techniczne, o gotowości świadczenia wymaganego serwisu (zawierające w szczególności: adres strony internetowej serwisu i numer infolinii telefonicznej).

Projekt współfinansowany przez Unię Europejską ze środków Pomocy Technicznej Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020 oraz z budżetu Samorządu Województwa Dolnośląskiego.

- Potwierdzenie posiadania inżynierów z certyfikatem NSE8 Fortinet Network Security Expert lub jego odpowiednikiem dedykowanym dla oferowanego rozwiązania
- 2 referencje w wysokości co najmniej 50 000 PLN brutto każda na dostarczenie systemów odpowiadających złożonej ofercie.
- Potwierdzenie posiadania ubezpieczenia OC na kwotę minimum 100 000 PLN brutto
- Certyfikat ISO 9001 podmiotu serwisującego.
- Oświadczanie, Producenta lub Autoryzowanego Dystrybutora na terytorium Polski, iż Wykonawca posiada autoryzację w zakresie sprzedaży oferowanych rozwiązań a oferowane produkty pochodzą z autoryzowanego kanału sprzedaży.
- W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), zostanie dołączony do oferty dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz.U.2023.1582 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

A.

Zakup 2 urządzeń zintegrowanej sprzętowej zapory sieciowej / router UTM klasy FortiGate 100F i FortiGate 60F + licencje FortiCare Premium i FortiGuard (UTP) na 3 lata lub innych równoważnych rozwiązań zapewniających pełną współpracę i integrację ze stosowanymi w instytucji rozwiązaniami FortiGate 50E i FortiClient, o następujących minimalnych wymaganiach sprzętowych, technicznych i funkcjonalnych:

Obszar	**Wymagania**	
	W stosunku do rozwiązania równoważnego do FortiGate 100F	**W stosunku do rozwiązania równoważnego do FortiGate 60F**
Wymagania ogólne	1. Zintegrowany system bezpieczeństwa dostarczający funkcjonalności: firewall, VPN, antywirus, IPS (ochrona przed atakami), filtrowanie treści WWW, ochrona przed spamem, kontrola aplikacji, optymalizacja pasma, kontroler sieci bezprzewodowych, mocne uwierzytelnianie. 2. Implementacja zarówno w trybie: routera z NAT'em, transparentnym realizującym wszystkie wymienione powyżej funkcje bezpieczeństwa oraz monitorowania na porcie SPAN. 3. System umożliwia 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. 4. System wspiera protokoły IPv4 oraz IPv6, co najmniej w zakresie: • Firewall; • Ochrony w warstwie aplikacji; • Protokołów routingu dynamicznego; 5. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łączy. 6. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i wszystkimi niezbędnymi licencjami.	
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub	

	Active-Passive. W obu trybach rozwiązanie zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.	
Interfejsy, Zasilanie	1. Oferowane rozwiązanie dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:	
Gigabit Ethernet RJ-45 (w tym m.in.: WAN/Internal/DMZ/ Management/HZ)	Minimum 16 portów	Minimum 10 portów
SFP 1 Gbps	Minimum 8 gniazda (w tym: co najmniej 4 dedykowane SFP; nie więcej niż połowa typu RJ45/SFP shared)	n/d
SFP+ 10 Gbps	Minimum 2 gniazda	n/d
	2. System posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC, z wtyczką obowiązującą na terytorium Polski.	
Parametry wydajnościowe		
Ilość jednoczesnych sesji (TCP)	Nie mniej niż 1,4 mln.	Nie mniej niż 700 tys.
Ilość nowych sesji/sekundę (TCP)	Nie mniej niż 52 tys.	Nie mniej niż 32 tys.
Przepustowość Firewall (512/64 byte UDP)	Minimum 18 / 10 Gbps	Minimum 10 / 6 Gbps
Opóźnienie Firewall (64 byte UDP packets)	Maksymalnie 6 µs	Maksymalnie 5 µs
Przepustowość Firewall (Packets Per Second)	Nie mniej niż 14 Mpps	Nie mniej niż 8 Mpps
Ilość polityk zapory	Minimum 9000	Minimum 4500
Wydajność szyfrowania IPSec VPN minimum protokołem AES z kluczem 128 (512 byte packet)	Minimum 11 Gbps	Minimum 6 Gbps
Ilość tuneli Gateway-to-Gateway IPSec VPN	Minimum 2000	Minimum 180
Ilość tuneli Client-to-Gateway IPSec VPN	Minimum 15000	Minimum 450
Max ilość użytkowników SSL-VPN Users	Minimum 450	Minimum 200
Przepustowość SSL-VPN	Minimum 750 Mbps	Minimum 750 Mbps
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach	Minimum 2,5 Gbps	Minimum 1,3 Gbps

modułu IPS) dla ruchu Enterprise Traffic Mix		
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus	Minimum 1,6-1Gbps	Minimum 650 Mbps
Przepustowość w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTP	Minimum 1 Gbps	Minimum 600 Mbps
Przepustowość kontroli aplikacji	Minimum 2,1 Gbps	Minimum 1,7 Gbps
Przepustowość Threat Protection	Minimum 950 Mbps	Minimum 700 Mbps
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych, zintegrowanych w jeden system: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada 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).	
	14. Analiza ruchu szyfrowanego protokołem SSH.	
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 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. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	

	4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. 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 vCenter (ESXi). • VMware NSX. • Kubernetes.	
Maksymalna Ilość polityk Firewall	Minimum 9000	Minimum 4500
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • 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 oraz 21. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • 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. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • 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.	
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę:	

Projekt współfinansowany przez Unię Europejską ze środków Pomocy Technicznej Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020 oraz z budżetu Samorządu Województwa Dolnośląskiego.

	1. Routingu statycznego. 2. Routing w oparciu o Polityki [Policy Based Routingu] (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). 3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu. 4. Rozwiązanie powinno wspierać funkcję Forward Error Correction na tunelach IPSec. 5. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.
Zarządzanie pasmem	1. Rozwiązanie umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. Rozwiązanie zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS. 3. 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. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. 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. Rozwiązanie Sandbox nie jest przedmiotem bieżącego zamówienia.

	8. System wstrzymuje dostarczenie pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox. 9. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 10. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 11. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. 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	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 mln adresów URL pogrupowanych w kategorie tematyczne. 2. 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. 3. Filtr WWW dostarcza kategorie stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

	5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. 11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo. 12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.
Uwierzytelnianie użytkowników w ramach sesji	1. Rozwiązanie 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. 2. System daje możliwość zastosowania uwierzytelniania dwuskładnikowego. 3. Rozwiązanie 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. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. 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. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

	9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie zdarzeń	1. 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. 2. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej 36 miesięcy. 3. 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. 4. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 5. Możliwość włączenia logowania per reguła w polityce firewall. 6. System zapewnia możliwość logowania do serwera SYSLOG. 7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu muszą być możliwe do zweryfikowania w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Wykonawca zapewnia wymagane licencje do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów na okres minimum 36 miesięcy, m.in. zakresie: Kontrola Aplikacji, IPS, Advanced Malware Protection, URL Filtering, DNS Filtering , Video Filtering, Antispam Service, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), oraz wsparcie techniczno-serwisowe odpowiadające swoim zakresem i poziomem FortiCare Premium. Wymagany jest poziom licencjonowania odpowiadający swoim zakresem co najmniej FortiGuard Unified Threat Protection
Gwarancja oraz wsparcie	1. Cały System jest objęty serwisem gwarancyjnym producenta przez okres minimum 36 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 co najmniej w trybie 8x5 . Wymagany serwis co najmniej w trybie 8x5. 2. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim co najmniej w trybie 8x5 przez dedykowany internetowy moduł serwisowy oraz infolinię w języku polskim. Czas reakcji na zdarzenia krytyczne jest nie dłuższy niż 1 godzina, a na zdarzenia nie-krytyczne jest nie dłuższy niż następny dzień roboczy – reakcja co najmniej w postaci połączenia telefonicznego lub odpowiedzi w dedykowanym portalu serwisowym.

B

Zakup działającego w środowisku wirtualnym centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń, klasy FortiAnalyzer-VM (Subscription license for 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service) z wsparciem na 3 lata lub innego równoważnego rozwiązania zapewniającego pełną współpracę i integrację z rozwiązaniem zaoferowanym w pkt. A oraz ze stosowanymi w instytucji rozwiązaniami FortiGate 50E i FortiClient, o następujących minimalnych wymaganiach technicznych i funkcjonalnych:

Obszar	**Wymagania** **W stosunku do rozwiązania równoważnego do FortiAnalyzer-VM**
Wymagania ogólne	1. Centralny system integrujący w sobie rejestrowanie/logowanie, analizę i raportowanie zdarzeń sieciowych, zapewniając większą wiedzę na temat bezpieczeństwa zdarzeń i incydentów w całej sieci. 2. Rozwiązanie zapewnia scentralizowaną analizę zdarzeń związanych z bezpieczeństwem, badania kryminalistyczne, raportowanie, archiwizację treści, eksplorację danych, kwarantannę złośliwych plików i ocenę podatności. Scentralizowane gromadzenie, korelację i analizę danych z rozwiązań zaproponowanych w pkt. A, rozwiązań Fortinet (FortiGate 50E, FortiClient) wykorzystywanych dotychczas przez Zamawiającego oraz urządzeń sieciowych innych producentów. 3. 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: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.
Interfejsy, Dysk	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 3 TB
Parametry wydajnościowe	1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów / urządzeń / VDOMs.
Logowanie zdarzeń	1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. 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. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. 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.

	6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długoczasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
Raportowanie	W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
Analiza i Korelacja logów	W zakresie analizy i korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi analizować i korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware; • Aplikacje sieciowe; • Email; • IPS; • Traffic; • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
Zarządzanie	1. Oferowane rozwiązanie musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczyć dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. • Proces uwierzytelniania administratorów musi być realizowany w oparciu co najmniej o: lokalną bazę, Radius, LDAP, PKI. 2. 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.
Gwarancja oraz wsparcie	Oferowane rozwiązanie musi być objęte licencją subskrypcyjną i serwisem producenta przez okres co najmniej 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego realizowanego co najmniej w trybie 8x5. Zgłoszenia serwisowe są przyjmowane w języku polskim co najmniej w trybie 8x5 przez dedykowany internetowy moduł serwisowy oraz infolinię w języku polskim.

Projekt współfinansowany przez Unię Europejską ze środków Pomocy Technicznej Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020 oraz z budżetu Samorządu Województwa Dolnośląskiego.