**Szczegółowy opis przedmiotu zamówienia**

**Wymagania techniczne dot. Systemu Zabezpieczeń dla Urzędu Marszałkowskiego Województwa Podlaskiego**

**Definicje:**

* SZ - System Zabezpieczeń składający się z FW SZ oraz dodatkowych urządzeń i systemów wspierających ich pracę.
* FW SZ – zapora ogniowa co najmniej typu NGFW, składająca się z minimum dwóch fizycznych zapór ogniowych pracujących w trybie niezawodnościowym, wchodząca w skład SZ.

|  |  |
| --- | --- |
| **Opis wymagania** | **Parametry minimalne** |
| 1. Wymagania ogólne
 | * 1. Dostawa FW SZ typu Next Generation Firewall (NGFW),
	2. Producent FW SZ, musi być uwzględniony w obszarze Leaders ewaluacji Gartnera 2021 Gartner® Magic Quadrant™ for Network Firewalls Magic Quadrant for Network Firewalls. Published 1 November 2021,
	3. FW SZ musi zostać dostarczony w postaci komercyjnej platformy,
	4. FW SZ musi umożliwiać uruchomienie go w dwóch niezależnych środowiskach w sposób umożliwiający zapewnienie wysokiej dostępności usług poprzez uruchomienie w każdym datacenter węzła klastra NGFW w trybie active-passive (HA).
		1. Dwa Datacenter oddalone od siebie o 1 km, między którymi rozpięte są ciemne włókna światłowodowe.
		2. Zarówno klaster jak i pojedyncze urządzenia (węzły klastra) muszą spełniać wszystkie opisane wymagania funkcjonalne oraz wydajnościowe.
	5. Poszczególne wymagania i parametry muszą być zrealizowane dla każdego z urządzeń fizycznych, tak aby wskazane parametry wydajnościowe zostały zachowane dla każdego datacenter w razie awarii lub niedostępności pojedynczego węzła klastra.
	6. Wszystkie dostarczane urządzenia FW SZ muszą być w tej samej konfiguracji i wersji.
	7. SZ musi być uruchomiony na urządzeniach o parametrach rekomendowanych przez producenta oprogramowania.
	8. Urządzenia:
		1. FW SZ muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
		2. Pozostałe urządzenia (inne niż FW SZ), muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie w okresie zapewnionej gwarancji muszą być objęte jego wsparciem.
	9. Urządzenia SZ muszą pochodzić z autoryzowanego kanału sprzedaży/dystrybucji producenta.
	10. SZ musi się składać z urządzeń fabrycznie nowych, nieużywanych i wolnych od wad fizycznych, w szczególności bez wad zmniejszających jego wartość lub użyteczność wynikającą z jego przeznaczenia;
	11. SZ musi być wolny od wad prawnych, a w szczególności nie stanowić własności osoby trzeciej ani nie może być obciążony jakimkolwiek prawem przysługującym osobie trzeciej, które wyłącza lub ogranicza możliwość przeniesienia prawa własności Sprzętu na Zamawiającego;
	12. SZ musi posiadać dołączone niezbędne instrukcje i materiały dotyczące użytkowania w języku polskim lub angielskim,
	13. SZ musi posiadać trwałe oznaczenia zawierające: nazwę producenta, typ, oznakowanie CE, numer fabryczny (o ile są przewidziane przez producenta)
	14. SZ jest kompatybilny i możliwy do wdrożenia w infrastrukturze teleinformatycznej Zamawiającego, a Wykonawca oświadcza, że zapoznał się z wykorzystywaną przez Zamawiającego technologią, w tym używanym sprzętem, oprogramowaniem, doprowadzonym zasilaniem, zabezpieczeniami, architekturą serwerową oraz sieciową, systemami operacyjnymi oraz że przedmiot umowy będzie prawidłowo funkcjonować w zakresie, w jakim to konieczne do realizacji przedmiotu umowy w kooperacji ze sprzętem i oprogramowaniem Zamawiającego przy uwzględnieniu zabezpieczeń wykorzystywanych przez Zamawiającego.
 |
| 1. Ogólne parametry fizyczne
 | * 1. FW SZ musi się składać z systemu połączonych, co najmniej dwóch dedykowanych, fizycznych urządzeń zabezpieczających sieć komputerową.
	2. FW SZ musi być w formie appliance’u fizycznego tj. odrębnej, niezależnej platformy sprzętowej.
	3. SZ musi być dedykowany przez producenta do montażu w 19” szafie RACK Zamawiającego.
	4. Uszkodzenie SZ musi być raportowane na urządzeniu w formie wizualnej np. dioda, wyświetlacz LCD itp.
 |
| 1. Zasilacze
 | * 1. Każde z urządzeń wchodzących w skład SZ musi być wyposażone w minimum dwa zasilacze zapewniające redundancję zasilania w trybie hot-plug.
	2. Połowa zainstalowanych zasilaczy musi zapewnić zasilanie wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości funkcjonalnych oraz wydajnościowych.
	3. Zasilacze muszą pracować z siecią energetyczną Zamawiającego o parametrach AC 230V, 50Hz.
 |
| 1. Interfejsy
 | * 1. Każde z urządzeń wchodzących w skład FW SZ musi być wyposażone w:
		1. Ilość: 16 interfejsów 10 Gbps SFP+, w tym:
			1. Ilość: 8 par wkładek światłowodowych SFP+W każdej parze musi być jedna wkładka kompatybilna z FW SZ, a druga z Cisco Nexus 5596 Zamawiającego.
			2. Ilość: 8 par wkładek światłowodowych SFP+W każdej parze musi być jedna wkładka kompatybilna z FW SZ, a druga z Cisco Nexus 5548UP Zamawiającego.
		2. Jeśli urządzenie nie ma wbudowanych portów QSFP 40 Gbps, to musi mieć możliwość rozbudowy o porty QSFP 40 Gpbs,
		3. 1 interfejs 1 Gbps wydzielony jako dedykowany do zarządzania out-of-band,
		4. 1 port konsolowy RJ45.
	2. FW SZ muszą obsługiwać agregowanie interfejsów fizycznych w obrębie pojedynczego węzła klastra
	3. Kable (patchcordy, kable zarządzające, konsolowe), wkładki i inne niewymienione, a niezbędne, muszą być dostarczone w ilości odpowiadającej liczbie interfejsów urządzenia i konfiguracji zgodnej z wdrożeniem w siedzibie Zamawiającego (adekwatna długość kabli, typ kabli, kategoria, technologia itp.)
	4. Wszelkie elementy programowe i sprzętowe, niezbędne do wdrożenia w siedzibie Zamawiającego oraz zrealizowania funkcjonalności SZ - muszą być dostarczone.
 |
| 1. Architektura systemu
 | * 1. Na SZ muszą składać się 2 fizyczne urządzenia typu appliance wykonujące kontrolę ruchu sieciowego.
	2. Dla urządzeń appliance (FW SZ) musi występować sprzętowa separacja modułu zarządzania i modułu przetwarzania danych.
	3. FW SZ musi umożliwiać podział na niezależne logiczne instancje.
		1. FW SZ musi umożliwiać uruchomienie minimum 10 w pełni funkcjonalnych, logicznych instancji systemu.
	4. FW SZ musi mieć możliwość zastąpienia obecnie pracujących fizycznych firewalli Zamawiającego tj:
		1. 2 urządzeń firewall wewnętrznego ruchu sieciowego pracujących w trybie active/standby,
		2. 1 urządzenia firewall wewnętrznego ruchu sieciowego
		3. 2 urządzeń firewall zewnętrznego ruchu sieciowego pracujących w trybie active/standby,
		4. 1 urządzenia firewall zewnętrznego ruchu sieciowego (styku z siecią Internet).
	5. Urządzenia fizyczne FW SZ muszą posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active/Standby.
	6. W przypadku klastra Active/Standby wymagane jest objecie licencjami całego klastra, czyli wszystkich urządzeń fizycznych wchodzących w skład FW SZ.
 |
| 1. Wydajność:
 | * 1. Każde z urządzeń tworzących FW SZ musi posiadać następujące parametry wydajnościowe dla przetwarzanego ruchu sieciowego:
		1. Całkowita wydajność urządzenia w trybie inspekcji Threat Prevention – rozumianym jako aktywna filtracja pakietów przy włączonych modułach bezpieczeństwa min. Firewall, Ochrona Antywirusowa, Ochrona Antymalware, Ochrona Antyspyware, System IPS, Identyfikacja i kontrola aplikacji, Filtracja Treści WWW/URL - nie mniejsza niż 20 Gbps.
		2. Maksymalna liczba obsługiwanych jednoczesnych połączeń - nie mniejsza niż 4 000 000 .
		3. Maksymalna liczba obsługiwanych nawiązywanych połączeń - nie mniejsza niż 200 000 / sek.
 |
| 1. Tryby pracy Systemu
 | * 1. System musi realizować zadania kontroli i filtracji ruchu sieciowego na poziomie co najmniej warstw: sieciowej, transportowej oraz aplikacyjnej modelu ISO-OSI za pomocą modułów:
		1. Firewall,
		2. System IPS,
		3. Identyfikacja i kontrola aplikacji,
		4. Ochrona Antywirusowa,
		5. Ochrona Antymalware,
		6. Ochrona Antyspyware,
		7. Filtracja Treści WWW/URL.
	2. System musi wspierać funkcjonalności, co najmniej:
		1. Realizacja połączeń VPN IPsec (Site-to-Site),
		2. Dostęp zdalny użytkowników (VPN)
		3. Inspekcja komunikacji szyfrowanej SSL/TLS (w tym TLS 1.3)
		4. Identyfikacja użytkowników,
		5. Filtracja sieci BOTNET oraz TOR,
		6. Translacja adresów,
		7. Protokoły routingu,
		8. Mechanizmy QoS,
		9. Sieci VLAN.
	3. FW SZ musi umożliwiać pracę w co najmniej 2 trybach:
		1. routera (tzn. w warstwie 3 modelu OSI),
		2. w trybie transparentnym.
	4. Praca w trybach wymienionych powyżej musi być możliwa również w ramach podziału na pojedyncze logiczne instancje systemu. Poszczególne instancje logiczne systemu muszą pracować niezależnie od siebie, w trybie routera lub w trybie transparentnym.
 |
| 1. Moduł kontroli ruchu sieciowego:

Firewall | * 1. FW SZ musi mieć możliwość zabezpieczeń typu firewall zgodnie z określoną polityką tj. musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci tj. strefami bezpieczeństwa na poziomie warstwy sieciowej, transportowej oraz aplikacji modelu ISO-OSI.
	2. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP, protokoły, usługi sieciowe, użytkowników oraz logowanie ruchu sieciowego.
	3. FW SZ musi zapewniać ochronę przed atakami typu DoS czy DDoS (flood protection).
	4. FW SZ musi zapewniać ochronę przed skanowaniem portów.
	5. FW SZ musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia pakietu (GeoIP).
 |
| 1. Moduł kontroli ruchu sieciowego:

System IPS | * 1. FW SZ musi posiadać moduł wykrywania i blokowania ataków intruzów opartego o sygnatury, zdefiniowane wzorce ruchu sieciowego oraz parametry protokołów sieciowych.
	2. Baza systemu IPS musi być regularnie aktualizowana w sposób automatyczny.
	3. Musi być możliwość edytowania reguł Systemu IPS.
	4. FW SZ musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.
	5. FW SZ musi generować alerty w przypadku wykrycia ataku.
	6. FW SZ musi zapewniać wykrywanie i blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command & Control (Advanced Threat Prevention).
 |
| 1. Moduł kontroli ruchu sieciowego:

Kontrola aplikacji | * 1. FW SZ musi obsługiwać mechanizm wykrywania aplikacji w ruchu sieciowym.
	2. FW SZ musi automatycznie identyfikować aplikacje bez względu na stosowane numery portów, protokoły i użyte szyfrowanie.
	3. Rozpoznanie aplikacji musi odbywać się co najmniej poprzez sygnatury.
 |
| 1. Moduł kontroli ruchu sieciowego:

Ochrona antywirusOchrona antimalwareOchrona antyspyware | * 1. FW SZ musi obsługiwać inspekcję ruchu pozwalającą na ochronę antywirusową, antimalware i antyspyware co najmniej dla protokołów: SMTP, POP3, HTTP i HTTPS oraz podstawowe rodzaje plików – minimum PDF, DOC, DOCX, XLS, XLSX, pliki wykonywalne oraz archiwa.
	2. Bazy modułów antywirusowego, antimalware i antyspyware muszą być aktualizowane w sposób automatyczny.
	3. System musi umożliwiać zablokowanie transferu plików w oparciu o ich rodzaj, protokół transmisji, kierunek transferu oraz zawierających złośliwy kod.
	4. Musi być możliwość edytowania reguł ochrony, antimalware oraz antyspyware.
 |
| 1. Moduł kontroli ruchu sieciowego:

Filtracja treści WWW/URL | * 1. FW SZ musi obsługiwać mechanizm filtrowania stron WWW, adresów URL w zależności od kategorii treści stron internetowych.
	2. FW SZ musi zapewnić możliwość dodania własnej kategorii.
	3. Baza kategorii stron musi być aktualizowana w sposób automatyczny.
	4. FW SZ powinien zapewniać skanowanie transferowanych plików w czasie rzeczywistym lub partiami.
	5. FW SZ powinien filtrować pliki na podstawie nagłówków.
	6. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania w nim logo organizacji.
 |
| 1. Wymagane funkcjonalności:

Realizacja połączeń VPN (site-to-site) | * 1. FW SZ musi obsługiwać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standard IPSec w konfiguracji site-to-site.
	2. FW SZ musi wspierać zestawianie zabezpieczonych kryptograficznie tuneli VPN dla logicznych instancji systemu.
 |
| 1. Wymagane funkcjonalności:

Dostęp zdalny VPN użytkowników (client-to-site) | * 1. FW SZ musi umożliwiać tworzenie tuneli client-to-site opartych o technologię SSL oraz IPsec.
	2. FW SZ umożliwia obsługę 100 użytkowników VPN jednocześnie.
	3. Użytkownicy zdalni muszą mieć możliwość autoryzowania się za pomocą: RADIUS, LDAP, certyfikatów, dwu-składnikowego uwierzytelniania bądź lokalnej bazy użytkowników.
	4. Klient VPN musi wspierać najnowsze systemy operacyjne: Windows, Android, iOS.
	5. FW SZ musi mieć możliwość wykorzystania portalu do uwierzytelniania użytkowników tzw. Captive Portal i uwierzytelniać ich w oparciu o LDAP.
 |
| 1. Wymagane funkcjonalności:

Inspekcja komunikacji szyfrowanej | * 1. FW SZ musi zapewniać inspekcję komunikacji szyfrowanej HTTPS dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników przeglądających zasoby w sieci Internet) oraz ruchu przychodzącego z sieci Internet do serwerów wewnętrznych (przeglądanie stron WWW Zamawiającego).
	2. FW SZ musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji Threat Prevention.
	3. FW SZ musi zapewnić możliwość wykluczenia z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL, dodania własnych wyjątków.
	4. Inspekcja ruchu musi dopuszczać analizę ruchu w trybie monitorowania (bez podjęcia reakcji).
 |
| 1. Wymagane funkcjonalności:

Identyfikacja użytkowników | * 1. FW SZ musi ustalać tożsamość użytkowników sieci w oparciu o Active Directory.
	2. Polityka kontroli dostępu (FW SZ) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet, gdy użytkownik zmieni lokalizację i adres IP.
	3. FW SZ nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów lub użytkowników w sieci wewnętrznej.
 |
| 1. Wymagane funkcjonalności:

Translacja adresów | * 1. FW SZ musi wykonywać statyczną i dynamiczną translację adresów NAT.
 |
| 1. Wymagane funkcjonalności:

Protokoły routingu | * 1. FW SZ musi zapewniać obsługę routingu statycznego.
	2. FW SZ musi zapewniać obsługę protokołów routingu dynamicznego BGP i OSPF.
	3. FW SZ musi zapewniać obsługę IGMP.
 |
| 1. Wymagane funkcjonalności:

Mechanizmy QoS | * 1. FW SZ musi zapewniać klasyfikację ważności ruchu pakietów na bazie:
		1. Protokołu sieciowego,
		2. Źródłowego i docelowego adresu IP,
		3. Numeru portu TCP lub UDP,
		4. Ustawienia pasma maksymalnego ruchu sieciowego (QoS),
		5. Tworzenie limitów ilości danych dla użytkowników w kierunku upload, download.
 |
| 1. Wymagane funkcjonalności:

Sieci VLAN | * 1. FW SZ musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q.
	2. FW SZ musi obsługiwać co najmniej 1024 znaczników VLAN.
	3. FW SZ musi obsługiwać ruch miedzy podsieciami VLAN.
 |
| 1. Zarządzanie:
 | * 1. Zarządzanie urządzeniami FW SZ musi odbywać się co najmniej: z linii poleceń (CLI) oraz graficznej konsoli Web (GUI) dostępnej przez przeglądarkę WWW.
	2. Interfejs SZ musi być w języku polskim lub angielskim.
	3. Dostęp do SZ i zarządzanie z sieci muszą być zabezpieczone kryptograficznie poprzez szyfrowanie komunikacji.
	4. SZ musi pozwalać na zdefiniowanie wielu administratorów o różnych poziomach uprawnień.
	5. Komunikacja FW SZ z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS, LDAP.
	6. FW SZ musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.
	7. FW SZ musi umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (OTP) lub tokena (U2F).
	8. Konsola zarządzająca, logująca i raportująca FW SZ musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji.
	9. FW SZ musi mieć wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego oraz do serwera FTP.
	10. FW SZ powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w zdefiniowanych odstępach czasowych.
	11. FW SZ musi mieć możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer, z możliwością wykorzystania ich do budowy polityk bezpieczeństwa.
	12. FW SZ powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.
	13. FW SZ musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
	14. FW SZ powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu zarządzania. Liczba takich prób oraz czas blokady muszą być definiowane przez administratora.
	15. FW SZ musi posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
 |
| 1. Logowanie i raportowanie:
 | * 1. SZ musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie.
	2. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
	3. Konsola zarządzająca musi umożliwiać generowanie raportów i przesyłania ich na wskazany adres e-mail.
	4. Logowanie działań administratora.
	5. SZ musi zapewniać monitorowanie w czasie rzeczywistym stanu SZ (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych, połączenia sieciowe, czas trwania połączeń sieciowych, liczba przesłanych danych, lista ‘top talkers’, lista ‘top attackers’, lista ‘top blocked connections’). Podobne statystyki powinny być dostępne również dla danych historycznych w ramach webowego interfejsu graficznego urządzenia.
	6. FW SZ musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.
	7. FW SZ musi mieć wsparcie dla protokołów:
		1. SNMP v1 lub v2 lub v3.
		2. Netflow lub jFlow lub NetStream lub cflowd lub IPFIX lub NSEL lub sFlow.
	8. SZ musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych celem długoterminowego przechowywania danych.
	9. W zakresie przeglądania logów i zdarzeń SZ musi zapewniać możliwość:
		1. przeglądanie zapisanych logów;
		2. przeglądanie zarchiwizowanych logów;
		3. filtrowanie logów co najmniej pod kątem:

- uwierzytelnionych użytkowników;- błędów w procesie uwierzytelniania użytkowników;- adresów źródłowych (IPv4, IPv6);- adresów docelowych (IPv4, IPv6);- połączeń odrzuconych, zablokowanych, przepuszczonych;- poszczególnych reguł polityki bezpieczeństwa.* 1. System musi posiadać funkcjonalność zbierania i przeglądania logów historycznych z SZ.
	2. SZ musi mieć możliwość przechowywania logów i zdarzeń SZ przez okres min. 2 lat bez konieczności archiwizacji.
	3. SZ musi mieć możliwość archiwizacji logów i zdarzeń.
	4. SZ musi mieć funkcjonalność centralnego zarządzania, logowania, raportowania, archiwizacji logów i zdarzeń SZ – niezależnie od urządzeń FW
	5. SZ musi mieć funkcjonalność analizy heurystycznej lub behawioralnej na podstawie zbieranych logów lub kopii ruchu sieciowego – niezależnie od urządzeń FW
 |
| 1. Zarządzanie
 | * 1. System musi posiadać funkcjonalność monitorowania stanu działania urządzeń SZ
	2. Wymagana jest konfiguracja zewnętrznego systemu monitorującego Zamawiającego np. Zabbix, Nagios itp. do monitoringu SZ.
	3. System musi posiadać funkcjonalność zarządzania konfiguracją i polityką bezpieczeństwa na urządzeniach
	4. Zarządzanie zdalne musi być realizowane z wykorzystaniem protokołów szyfrowanych (SSH, HTTPS). W przypadku gdy zarządzanie odbywa się przy wykorzystaniu protokołów nieszyfrowanych (telnet, HTTP) musi być możliwość wyłączenia tych protokołów.
	5. Musi być możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego do podsystemu konsoli zarządzania
	6. SZ musi zapewnić poprzez graficzny interfejs konfigurację polityk bezpieczeństwa i polityk ochrony IPS, routingów i konfiguracji tuneli IPSec
	7. SZ powinien zapewnić wersjonowanie konfiguracji urządzeń, porównywanie wersji i przywracanie konfiguracji urządzeń do wybranej wersji
	8. Administratorzy muszą mieć do dyspozycji mechanizm odtwarzania systemu i przywracania konfiguracji z kopii zapasowych. Wymaganie dotyczy zarówno konfiguracji urządzeń wirtualnych zarządzanych jak i samego systemu zarządzania.
	9. Musi być przygotowana procedura w formie papierowej lub elektronicznej dotycząca pełnego odtworzenia SZ z kopii bezpieczeństwa.
 |
| 1. API
 | * 1. System musi udostępniać API do konfiguracji urządzeń w celu integracji z innymi systemami.
	2. API musi być uwierzytelniane
	3. SZ musi być przygotowany na automatyczny import reguł do ACL z tekstowego pliku zewnętrznego udostępnionego przez Zamawiającego
	4. SZ musi umożliwiać automatyczny import z pliku tekstowego wykazu zakazanych domen internetowych
	5. Zamawiający otrzyma procedurę papierową lub elektroniczną dotyczącą konfiguracji API i definiowania automatycznego importu reguł.
 |
| 1. Gwarancja:
 | * 1. Wykonawca musi zapewnić gwarancję SZ przez okres 60 miesięcy od dnia podpisania końcowego protokołu odbioru.
	2. W czasie świadczenia gwarancji na SZ musi zostać zapewnione:
		1. dostęp do aktualizacji, najnowszych wersji oprogramowania, aktualnych sygnatur IPS/IDS/AV/URL, dostęp do bazy wiedzy, serwis producenta gwarantujący naprawę zgłoszonych błędów, przewodników konfiguracyjnych i narzędzi diagnostycznych w trybie 24x7
		2. serwis wszystkich elementów sprzętowych SZ łącznie z wymianą urządzeń na nowe w przypadku awarii w trybie 5x8 NBD on-site.
		3. serwis wszystkich elementów programowych SZ w trybie 5x8 NBD.
		4. W sytuacji uszkodzenia dysku twardego w jakimkolwiek elemencie SZ i konieczności jego wymiany gwarancyjnej - dysk twardy pozostaje u Zamawiającego.
		5. SZ musi mieć zaimplementowany RAID jako nadmiarowość dysków.
		6. Obsługa zgłoszeń serwisowych przez inżynierów Producenta.
		7. Dostęp do pomocy technicznej producenta.
		8. Pomoc techniczna z SZ musi być dostępna w Polsce i świadczona w języku polskim lub angielskim.
		9. SZ nie może posiadać ograniczeń licencyjnych dotyczących wydajności.
		10. SZ musi mieć pełne pokrycie licencyjne funkcjonalności w okresie gwarancyjnym.
		11. System musi być dostarczony w modelu „na własność” tj. brak odnowienia licencji, subskrypcji itp. wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania lub sygnatur.
		12. W przypadku uszkodzenia Wykonawca dostarczy urządzenia fabrycznie nowe, aktualnie obecne w linii produktowej producenta. W przypadku braku możliwości wymiany elementu/ podzespołu/ modułu, Wykonawca wymieni cały sprzęt na nowy; Wymienione urządzenie musi być o parametrach nie gorszych niż uszkodzone urządzenie, kompatybilne z SZ Zamawiającego.
		13. W czasie świadczenia gwarancji, żadne z urządzeń składających się na SZ nie może utracić wsparcia producenta.
		14. Urządzenia SZ muszą pochodzić z autoryzowanego kanału sprzedaży producenta.
		15. Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie terminu gwarancji, jeżeli reklamował wadę przed upływem tego terminu.
		16. Maksymalny czas reakcji serwisu:
		17. dotyczącego warstwy sprzętowej: NBD – następny dzień roboczy
		18. dotyczącego warstwy programowej (w tym konfiguracyjnej): NBD – następny dzień roboczy
		19. Maksymalny czas usunięcia awarii:
		20. dotyczącej warstwy sprzętowej jednego z urządzeń FW: 10 dni
		21. dotyczącej warstwy sprzętowej obu jednocześnie urządzeń FW: NBD – następny dzień roboczy
		22. dotyczącej warstwy programowej (w tym konfiguracyjnej), uniemożliwiającej pracę sieci komputerowej Zamawiającego lub świadczenie usług informatycznych, określoną przez Zamawiającego jako:awarię krytyczną: NBD – następny dzień roboczy
		23. dotyczącej warstwy programowej (w tym konfiguracyjnej), nie mającej wpływu na ciągłość świadczenia usług Zamawiającego, określoną przez Zamawiającego jako: awarię niekrytyczną: 10 dni
 |
| 1. Reputacja
 | * 1. Potwierdzenie znajdowania się producenta FW SZ w kwadracie Leaders raportu Gartnera musi być dostarczone w dokumentacji.
 |
| 1. Dodatkowe wymagania
 | * 1. Wszelkie wymagane komponenty (kable, listwy, wkładki, interfejsy, karty, moduły, szyny, licencje, patchcordy itp.) niezbędne do uruchomienia SZ i podłączenia do infrastruktury Zamawiającego muszą być dostarczone w ramach przedmiotu zamówienia i kompatybilne z infrastrukturą Zamawiającego.
 |
| 1. Szkolenia:
 | * 1. W ramach realizacji Umowy Wykonawca zapewni uczestnictwo w autoryzowanych przez producenta szkoleniach w zakresie podstawowej i zaawansowanej konfiguracji SZ zakończone autoryzowanym egzaminem wiedzy co najmniej trzech pracowników Zamawiającego, w terminie zaakceptowanym przez Zamawiającego.
	2. Wykonawca dostarczy autoryzowane materiały szkoleniowe w języku polskim lub angielskim.
	3. W przypadku, gdy Wykonawca zaproponuje przeprowadzenie szkolenia poza miejscem realizacji umowy tj. poza siedzibą (miejscowością) Zamawiającego jest zobowiązany do zapewnienia dojazdu do tego miejsca, zakwaterowanie uczestników, ich wyżywienie oraz powrót.
	4. Szkolenia z SZ muszą być przeprowadzone w języku polskim na terenie RP.
	5. Szkolenia z SZ muszą zostać przeprowadzone i zakończone przed podpisaniem końcowego protokołu odbioru umowy.
	6. Jeśli pracownik Zamawiającego nie będzie mógł uczestniczyć w szkoleniu, wówczas będzie mógł zamienić szkolenie na voucher/talon/grant do wykorzystania przez Zamawiającego w odpowiadającym mu terminie.
 |
| 1. Wymagania dotyczące instalacji, konfiguracji i integracji urządzeń.Wdrożenie.
 | * 1. Wykonanie i przedstawienie do akceptacji Zamawiającego projektu wdrożenia SZ.
	2. Montaż urządzeń w szafie RACK wskazanej przez Zamawiającego. Montaż urządzeń FW SZ będzie polegał na instalacji FW SZ w dwóch budynkach Zamawiającego, oddalonych od siebie w odległości ok. 1 km i połączonych ze sobą ciemnymi włóknami światłowodowymi.
	3. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.
	4. Konfiguracja klastra niezawodnościowego pracującego w trybie active-passive.
	5. Konfiguracja podstawowych ustawień systemowych: serwer czasu, DNS, adres interfejsu zarządzającego, konto administracyjne.
	6. Wykonanie projektu technicznego w zakresie wyodrębnienia i skonfigurowania logicznych instancji firewall. Po akceptacji Zamawiającego, przeniesienie konfiguracji fizycznych firewalli do logicznych instancji firewall.
	7. Przeniesienie i modyfikacja konfiguracji z obecnych urządzeń zabezpieczeń do wdrażanego SZ. Na etapie wdrożenia Zamawiający wspólnie z Wykonawcą określą zaakceptowane przez obie strony: plan, poszczególne etapy i sposób wdrożenia mając na względzie bezpieczeństwo, ciągłość działania świadczonych usług i czas wdrożenia w danym momencie.
	8. Odwzorowanie konfiguracji obecnie używanych urządzeń bezpieczeństwa w zakresie:
		1. Konfiguracji interfejsów sieciowych oraz tras routingu w poszczególnych logicznych instancjach.
		2. Obiektów wraz z przypisanymi im adresami IP w poszczególnych logicznych instancjach.
		3. Polityk bezpieczeństwa firewall (L4) oraz konfiguracji NAT w poszczególnych logicznych instancjach.
		4. Bazy użytkowników dla autoryzacji połączeń zdalnych.
		5. Identyfikacji użytkowników poprzez domenę Active Directory.
	9. Aktywacja wymaganych licencji oraz konfiguracja pobierania aktualizacji baz dla modułów bezpieczeństwa.
	10. Konfiguracja modułów bezpieczeństwa dla analizy i ochrony ruchu przychodzącego z sieci Internet do zasobów wewnętrznych.
		1. Blokowanie ruchu z adresów IP na podstawie reputacji i geolokalizacji.
		2. Blokowanie ruchu sieciowego na podstawie sygnatur IPS,
		3. Blokowanie ruchu sieciowego poprzez wykorzystanie API do automatycznego importu reguł
	11. Konfiguracja modułów bezpieczeństwa dla analizy i ochrony ruchu wychodzącego z sieci wewnętrznej.
		1. Blokowanie niedozwolonych treści WWW.
		2. Blokowanie niedozwolonych aplikacji i protokołów sieciowych.
		3. Skanowanie ruchu w celu zapobieganiu złośliwemu oprogramowaniu (antymalware, antywirus).
	12. Konfiguracja raportów z ruchu sieciowego użytkowników.
	13. Konfiguracja raportów dotyczących ruchu przychodzącego z sieci Internet.
	14. Konfiguracja bramy umożliwiającej dostęp VPN dla użytkowników zdalnych.
	15. Konfiguracja automatycznej kopii zapasowej SZ według określonego harmonogramu.
	16. Zamawiający wymaga przeprowadzenia prac wdrożeniowych SZ ma miejscu. W przypadku części prac, gdy Zamawiający uzna, że mogą być realizowane zdalnie – wówczas zezwoli na dedykowany do tego celu kanał komunikacyjny.
 |
| 1. Dokumentacja
 | * 1. Dokumentacja powykonawcza musi odzwierciedlać stan faktyczny SZ w momencie zakończenia prac wdrożeniowych. Musi zawierać m.in.:
		1. Opis architektury połączeń fizycznych.
		2. Opis architektury topologii logicznej sieci.
		3. Opis uruchomionych modułów kontroli ruchu sieciowego wraz ze zdefiniowanymi politykami.
		4. Opis skonfigurowanych wymaganych funkcjonalności podczas wdrożenia.
		5. Opis wdrożonego systemu zarzadzania oraz raportowania zdarzeń wraz ze zdefiniowanymi raportami.
	2. Dokumentacja musi być wykonana w formie minimum elektronicznej.
	3. Zamawiający wymaga przygotowania przez Wykonawcę min. 20 procedur obsługi dotyczących SZ.
	4. Zamawiający wymaga udokumentowania parametrów technicznych i wymaganych funkcjonalności SZ poprzez karty katalogowe producenta urządzeń lub oświadczenie producenta urządzenia/oprogramowania.
 |
| 1. Licencje/Subskrypcje
 | * 1. W ramach postępowania muszą zostać dostarczone subskrypcje na okres 60 miesięcy od podpisania końcowego protokołu odbioru, upoważniające do aktualizacji SZ oraz korzystania z aktualnych baz sygnatur. Subskrypcje baz sygnatur powinny obejmować co najmniej moduły: Kontrola Aplikacji, IPS, Antywirus, Web Filtering
	2. Licencje na SZ nie mogą mieć ograniczeń czasowych (licencje wieczyste) z zastrzeżeniem, że nie dotyczy to licencji subskrypcyjnych, o których mowa powyżej.
	3. System musi być dostarczony z licencjami umożliwiającymi zarządzanie wszystkimi zaoferowanymi w ramach Systemu urządzeniami wirtualnymi NGFW
 |