Załącznik nr 1 f do OPZ Firewall mały

**Firewall** – Miasto Bielsk Podlaski, Miasto Grajewo, Gmina Krasnopol, Gmina Drohiczyn, Gmina Siemiatycze, Gmina Milejczyce, Gmina Sokółka, Gmina Suchowola, Gmina Nowe Piekuty – dla każdego partnera szt.1

|  |  |
| --- | --- |
| **ARCHITEKTURA SYSTEMU OCHRONY** | |
| **Typ systemu ochrony** | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge). |
| **Wymagania systemowe** | System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.  Obsługa nielimitowanej ilości hostów w sieci chronionej.  Minimalna liczba i typ interfejsów fizycznych: 4x GE (IEEE 1000Base-T), 2x GE (IEEE 1000Base-X), 2x USB 3.0 (Type-A), 1x Console (RJ-45 lub DB9) z możliwością rozbudowy o co najmniej 8 x GE (IEEE 1000Base-T lub IEEE1000Base-X).  Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)  Minimalna liczba nowych połączeń na sekundę: 80 000  Minimalna liczba jednoczesnych połączeń: 6 500 000  Minimalna przepustowość Firewall (IMIX): 12 000 Mbps  Minimalna przepustowość IPS: 4 000 Mbps  Minimalna przepustowość Web Proxy AV: 2 000 Mbps  Minimalna przepustowość IPSec: 1 800 Mbps  Minimalna liczba równoczesnych tuneli IPSec VPN: 1 300  Minimalna liczba równoczesnych tuneli SSL VPN: 300  Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB.  Możliwość rozbudowy o redundantny zasilacz sieciowy. |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** | |
| **Zarządzanie i utrzymanie** | Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).  Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup.  Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.  Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.  System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud.  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email.  Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.  Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.  Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.  Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).  System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.  W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.  System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.  Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.  System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).  System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).  System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  Rozwiązanie powinno zapewniać obsługę routingu statycznego.  Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).  Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).  System powinien oferować wsparcie dla IGMP snooping.  Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy).  Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.  System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.  Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.  Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.  Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).  System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.  System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.  Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. |
|  |  |
| **Autoryzacja użytkowników** | Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.  System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.  Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password).  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.  Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal. |
| **Samoobsługowy portal dla użytkowników** | Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.  Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).  Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.  Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.  Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.  Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email. |
| **Podstawowe opcje VPN** | System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:  Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)  Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). |
| **Klient IPSec VPN** | Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.  Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.  Wsparcie dla split-tunneling.  Wsparcie dla NAT-traversal.  Monitorowanie stanu połączenia. |
| **OCHRONA SIECI** | |
| **IPS** | Moduł ochrony klasy IPS z bazą minimum 7000 sygnatur.  Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.  Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.  System powinien generować alerty w przypadku wykrycia ataku. |
| **ATP** | System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control. |
| **Clientless VPN** | Udostępnianie zasobów w postaci usługRDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5. |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** | |
| **Ochrona i kontrola Web** | Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.  Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).  System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.  System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego.  Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).  Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).  Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.  System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.  System powinien zapewniać możliwość emulacji skryptów JavaScript.  Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.  Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.  Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać blokadę stron HTTPS.  Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji. |
| **Ochrona i kontrola aplikacji** | Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.  Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.  Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.  Rozwiązanie powinno umożliwiać blokowanie:  - aplikacji, które pozwalają na transfer plików (np. P2P).  - komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.  - proxy uruchamianych poprzez przeglądarki internetowe.  - streaming media (radio internetowe, Youtube, Vimeo).  Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo. |
| **Kształtowanie pasma dla Web i Aplikacji** | Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.  Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.  Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared). |
| **OCHRONA I KONTROLA EMAIL** | |
| **Ochrona i kontrola Email** | Rozwiązanie powinno oferować możliwość wyboru trybu pracy: Transparent Email Proxy lub Explicit Email Proxy (jako MTA).  System powinien umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS.  Rozwiązanie powinno zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.  System powinien umożliwiać uruchomienie drugiego niezależnego silnika antywirusowego.  Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur zagrożeń.  System powinien zapewniać wykrywanie, blokowanie i skanowanie załączników.  Rozwiązanie musi umożliwiać akceptowanie lub odrzucanie wiadomości przekraczających określony przez administratora rozmiar.  System powinien wykrywać próby phishingu przez analizę adresów URL zamieszczanych w treści wiadomości.  Rozwiązanie powinno oferować ochronę przed wyciekiem danych (DLP) na podstawie predefiniowanych wzorców lub kryteriów zdefiniowanych przez administratora.  System powinien oferować mechanizm analizy ruchu szyfrowanego TLS dla SMTP, POP oraz IMAP.  Rozwiązanie powinno umożliwiać dodanie stopki do każdej wiadomości wychodzącej.  Rozwiązanie powinno umożliwiać archiwizowanie wiadomości email.  Rozwiązanie powinno współpracować z co najmniej dwoma bazami RBL.  Rozwiązanie powinno umożliwiać tworzenie białych i czarnych list adresów IP i email.  Rozwiązanie powinno zapewniać wykrywanie spamu niezależnie od stosowanego języka.  Rozwiązanie powinno blokować spam w postaci plików graficznych np. wiadomości z tekstem osadzonym w obrazku. |
| **Kwarantanna Email** | System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako spam z opcją powiadamiania użytkownika.  System powinien zapewniać wbudowany system kwarantanny dla wiadomości sklasyfikowanych jako zainfekowane przez malware.  Rozwiązanie powinno zapewniać możliwość przeglądania kwarantanny z opcją wyszukiwania wiadomości i opcjami filtrowania po dacie, nadawcy, odbiorcy, temacie wraz z opcją zwalniania lub usuwania wiadomości z kwarantanny (przez samoobsługowy portal użytkownika). |
| **LOGOWANIE I RAPORTOWANIE** | |
| **Logowanie i raportowanie** | System musi umożliwiać składowanie oraz archiwizację logów za pomocą wbudowanego i bezpłatnego mechanizmu o cechach analizatora ruchu, posiadającego również funkcję integracji z zewnętrznym oprogramowaniem Producenta.  System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.  System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.  System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno generować raporty w PDF, HTML i XLS.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.  System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji. |
| **POZOSTAŁE** | |
| **Certyfikaty** | CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC, Common Criteria EAL4+, ICSA Labs Corporate Firewall |
| **Subskrypcje** | Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 36 miesięcy |
| **Gwarancja i wsparcie** | Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż  Gwarancja na sprzęt na okres nie krótszy niż 36 miesięcy  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. |
| **Instalacja** | Wykonawca wykona instalację i uruchomienie sprzętu wg wymagań Zamawiającego. |