*Załącznik nr 5*

**Specyfikacja techniczna sprzętu komputerowego i usług objętych zamówieniem**

**Modernizacja infrastruktury informatycznej oddziału WFOŚiGW
we Wrocławiu – Etap III**

# Struktura systemu informatycznego WFOŚiGW we Wrocławiu (stan aktualny).

W centrali Funduszu we Wrocławiu zainstalowane są 3 serwery fizyczne, 3 wirtualne i 42 stacje robocze pracujące w większości pod systemami Windows 7. W celu zachowania ciągłości działania aplikacji produkcyjnych, poczty i systemów operacyjnych, w I i II etapie modernizacji infrastruktury informatycznej WFOŚiGW we Wrocławiu, utworzono klaster niezawodnościowy złożony z dwóch serwerów Dell R320 oraz macierzy Dell serii PowerVault MD 3420. Klaster zbudowany jest w oparciu o system Windows Sewer 2012 R2.
W pozostałych oddziałach firmy pracują pojedyncze serwery spełniające jedynie rolę serwerów plików i kontrolerów domeny. Większość z 40 stacji roboczych, pracujących
w oddziałach, korzysta ze zdalnego dostępu do systemów produkcyjnych i ich baz znajdujących się na serwerach we Wrocławiu. Oddziały zewnętrzne Funduszu spięte są
z centralą we Wrocławiu kanałami VPN.

# Główny cel projektu i zakres prac

Głównym celem etapu III jest poprawa bezpieczeństwa całej sieci firmowej na styku z Internetem i poprawa komunikacji między oddziałami Funduszu poprzez wymianę aktualnie posiadanych routerów Cisco na urzadzenia klasy UTM NG firewall. Urządzenia powinny spełniać wymagania opisane w pkt. 4. Dodatkowo wykonawca zapewni w ramach umowy usługę wsparcia technicznego na całe środowisko serwerowe na warunkach opisanych w pkt. 3.

# Zakres prac instalacyjnych

1. Dostawa urządzeń UTM NG firewall do siedziby Zamawiającego,
2. Aktualizacja dostarczonych urządzeń do najnowszych wersji Firmware oraz aktywizacja licencji,
3. Instalacja, konfiguracja i uruchomienie urządzenia w centrali Zamawiającego (Wrocław),
4. Instalacja, konfiguracja i uruchomienie w oddziale Zamawiającego (Legnica)
5. Wstępna konfiguracja urządzeń dla oddziałów w Jeleniej Górze i Szczawnie Zdroju, umożliwiająca podłączenie i uruchomienie urządzenia na miejscu przez lokalnego informatyka,
6. Asysta zdalna przy uruchomieniu urządzeń w oddziałach w Jeleniej Górze i Szczawnie Zdroju.

# Konfiguracja i uruchomienie systemu

1. Konfiguracja wszystkich urządzeń w sposób odzwierciedlający konfigurację obecnie używanych Firewalli w tym konfiguracji sieciowej,
2. Strojenie systemu w niezbędnym zakresie,
3. Przeprowadzenie testów akceptacyjnych,
4. Przełączenie całości ruchu z obecnego Firewalla na nowy system,
5. Podłączenie wszystkich urządzeń do Usługi Centralnego Zarządzania (jeśli została zaoferowana),
6. Konfiguracja i uruchomienie kanałów VPN pomiędzy centralą Zamawiającego
a wszystkimi oddziałami,
7. Konfigurację mechanizmu raportowania dla urządzenia w Centrali,
8. Konfiguracja dodatkowych usług na wszystkich dostarczonych urządzeniach:
	1. Konfiguracja QoS dla uzgodnionych z Zamawiającym aplikacji,
	2. Konfiguracja ochrony antywirusowej w tym ochrony wewnętrznego serwera pocztowego,
	3. Konfiguracja mechanizmu kontroli aplikacji,
	4. Konfiguracja reguł Firewalla,
	5. Uruchomienie i konfiguracja kategoryzowania stron,
	6. Konfiguracja i dostrojenie mechanizmu IPS ,
	7. Konfiguracja i dostrojenie mechanizmu ATD,
	8. Integracja urządzeń z kontrolerami AD w centrali oraz oddziałach.

# Przygotowanie i przekazanie dokumentacji powykonawczej

1. Konfigurację systemu,
2. Instrukcję obsługi urządzeń UTM NG firewall,
3. Procedury awaryjne,
4. Procedury zgłoszeń serwisowych.

# Zamawiane wsparcie

W ramach zamówienia Wykonawca będzie świadczył wsparcie techniczne
i administracyjne w okresie **36 miesięcy** od daty podpisania protokołu odbioru etapu III
z umownym limitem **100 godzin** do wykorzystania w dowolnym okresie trwania mowy.

## Zakres realizowanego wsparcia

Wykonawca w ramach wsparcia będzie realizował prace serwisowe, konserwacyjne oraz inne usługi administracyjne zgłoszone przez Zamawiającego w zakresie objętym wsparciem.

Realizowane wsparcie dotyczy całej infrastruktury serwerowo-sieciowej zamawiającego zlokalizowanej w siedzibie Zamawiającego we Wrocławiu.

Infrastruktura objęta wsparciem składa się z 4 dostarczonych w ramach tego postępowania NG Firewalli, 3 serwerów fizycznych DELL, paru serwerów wirtualnych opartych o system Windows Server, jednej macierzy Dell PowerVault MD, 2 UPSów APC, dwóch routerów CISCO i dwóch przełączników LAN.

Szczegółowa dokumentacja infrastruktury IT zostanie udostępniona przez zamawiającego po wyłonieniu Wykonawcy i podpisaniu umowy.

W ramach serwisu Wykonawca będzie także reprezentował Zamawiającego przed producentami urządzeń sieciowo-serwerowych i w jego imieniu nadzorował cały proces gwarancyjny. Reprezentacja ta dotyczy tylko urządzeń objętych obecnie wsparciem producenta.

## Zgłaszania żądań obsługi

Na wypadek awarii i zgłoszeń pilnych Wykonawca umożliwi Zamawiającemu realizację zgłoszeń poprzez dedykowaną linię telefoniczną. Dodatkowym atutem będzie umożliwienie Zamawiającemu zgłaszania żądań usługi wsparcia również poprzez dedykowany portal on-line na stronie www Wykonawcy. W takim przypadku Zamawiający oczekuje aby udostępniony portal on-line posiadał następujące funkcjonalności, niezbędne m.in. do właściwego dokumentowania realizowanych prac:

* zgłaszanie żądania usługi lub niesprawności systemu,
* wgląd w status obecnego zgłoszenia,
* wgląd w historię zgłoszeń, ich stan, czas realizacji oraz informacje o osobach realizujących żądania.

## Wymagania SLA

Zamawiający w celu zapewnienia ciągłości swojej pracy biznesowej wymaga od Wykonawcy:

* Możliwość zgłaszania awarii i niesprawności systemu telefonicznie w trybie 5x9 (przez 5 dni roboczych w tygodniu w godzinach 7-16) z czasem reakcji 4 godziny od zgłoszenia
* Możliwość zgłaszania żądań usługi w trybie on-line w dowolnym czasie z czasem reakcji 4 godziny w trybie 5x9 (przez 5 dni roboczych w tygodniu w godzinach 7-16), w przypadku udostępnienia Zamawiającemu portalu on-line opisanego w pkt. 3.2.

Jako czas reakcji rozumie się tutaj ustalenie stron co do terminu, szczegółowego zakresu prac i czasochłonności prac.

W przypadku awarii Wykonawca zobowiązuje się do możliwie najszybszego przywrócenia pracy systemu i urządzeń w zależności od typu awarii.

# Tabela specyfikacji sprzętowej

|  |  |
| --- | --- |
|  | **Wymogi dotyczące NG Firewalla** |
| L.p. | Wymagane minimalne parametry techniczne | Parametry techniczne oferowanego urządzenia(wypełnia Wykonawca) |
| **A** | **B** | **C** |
| 1 | Oferowane rozwiązanie musi być dostępne jako platforma sprzętowa oraz musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać od użytkownika instalacji osobnego systemu operacyjnego |  |
| ……………………………………………………………………/wpisać: model, symbol, producent urządzenia/ |
| 2 | Rozwiązanie musi łączyć w sobie:·    zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),·    system IPS/IDS,·    filtr warstwy 7 wraz z obsługą SSL Interception·    serwer VPN,·    HTTP Proxy, wraz z kategoriami tematycznymi (minimum 80 kategorii),·    filtr antywirusowy. |
|
|
|
|
|
|
| 3 | Oferowane rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania, bez restartowania rozwiązania. |
| 4 | Oferowane rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów. |
| 5 | Oferowane rozwiązanie musi obsługiwać:·       NAT, PAT, proxy arp, VLAN,·       Protokoły VoIP – H.323, SIP, SCCP,·       Protokoły OSPF, RIP, BGP zarówno przy połączeniach IP jak i VPN. |
|
|
|
| 6 | Oferowane rozwiązanie musi posiadać funkcję Access Pointu Wi-Fi i obsługiwać standard 802.11glub wyższy z prędkością minimum 300Mb. | …………………………………………………………/podać: standard i maks. prędkość oferowanego Access Pointu/ |
| 7 | Oferowane rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk musi być nie większe niż 10 sekund. |
| 8 | Oferowane rozwiązanie musi posiadać możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym). |
| 9 | Oferowane rozwiązanie musi umożliwiać ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym). |
| 10 | Oferowane rozwiązanie musi posiadać watchdoga sprawdzającego w czasie rzeczywistym status działających usług, stanu łącz internetowych, czy statusu switchy obsługujących SNMP. |
| 11 | Oferowane rozwiązanie musi posiadać licencję na nielimitowaną liczbę użytkowników Firewalla |
| 12 | Oferowane rozwiązanie musi zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius.Ponadto, rozwiązanie musi zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN, proxy HTTP (działające na wielu procesorach), proxy FTP, proxy SSH oraz uwierzytelnianie administratorów. |
|
| 13 | Oferowane rozwiązanie musi zapewniać możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive i Active-Active. Urządzenie musi pozwalać na stworzenie dedykowanego linku, służącego tylko do monitorowania stanu partnera w klastrze High Availability. |
|
| 14 | Oferowane rozwiązanie musi mieć możliwość łączenia wielu kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości, wraz z obsługą protokołu LACP. |
| 15 | Oferowane rozwiązanie musi umożliwiać obsługę kart UMTS/EDGE/HSDPA. Jako łącza zapasowego |
| 16 | Oferowane rozwiązanie musi zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI. |
| 17 | Oferowane rozwiązanie musi posiadać firewall, obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu. |
| 18 | Oferowane rozwiązanie musi umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy. |
| 19 | Oferowane rozwiązanie musi pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router). |
| 20 | Oferowane rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej na firewallu. |
| 21 | Oferowane rozwiązanie musi umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia. |
| 22 | Oferowane rozwiązanie musi umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie. |
| 23 | Oferowane rozwiązanie musi umożliwiać tworzenie dynamicznych reguł firewalla uruchamianych z interfejsu SSL VPN. |
| 24 | Oferowane rozwiązanie musi posiadać wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika i z CLI. |
| 25 | Oferowane rozwiązanie musi posiadać wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu. |
| 26 | Oferowane rozwiązanie musi posiadać zintegrowany filtr warstwy 7 |
| 27 | Oferowane rozwiązanie musi umożliwiać przechwytywanie i rozszyfrowywanie ruchu SSL/TLS |
| 28 | Oferowane rozwiązanie musi pozwalać na blokowanie pojedynczych funkcji konkretnych aplikacji (np. blokowanie tylko transferu plików w Gadu-Gadu, blokowania tylko funkcji czata czy też wybranych gier na portalu facebook lub przepuszczania tylko i wyłącznie aktualizacji programów pracujących w sieci. |
| 29 | Oferowane rozwiązanie musi posiadać protokół dla tuneli VPN site-to-site i client-to-site. |
| 30 | Oferowane rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN. |
| 31 | Oferowane rozwiązanie musi zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji |
| 32 | Oferowane rozwiązanie musi obsługiwać multitransport VPN – tworzenie do min. 20 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień. |
| 33 | Oferowane rozwiązanie musi zapewnić możliwość łączenia transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych. |
| 34 | Oferowane rozwiązanie musi umożliwiać przypisywanie ruchu do wybranego transportu VPN w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia i godziny nawiązania połączenia. |
|
| 35 | Oferowane rozwiązanie musi zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP. |
| 36 | Oferowane rozwiązanie musi posiadać w standardzie, darmowego klienta NAC integrującego się z centrum akcji w systemach Windows 7/8/10. |
| 37 | Oferowane rozwiązanie musi zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS. |
| 38 | Oferowane rozwiązanie musi umożliwiać tworzenie kanałów VPN (client-2-site) wykorzystując wbudowany w Windows 7/8/10 mechanizm tworzenia połączeń VPN (bez aplikacji firm trzecich) |
| 39 | Oferowane rozwiązanie musi zapewniać centrum autentykacji i autoryzacji na lokalnym serwerze VPN. |
| 40 | Oferowane rozwiązanie musi umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania. |
| 41 | Oferowane rozwiązanie musi zapewniać obsługę urządzeń kryptograficznych (tokenów, kart) współpracujących z mechanizmem Microsoft Strong Credential Provider dla systemu Windows. |
| 42 | Oferowany w ramach rozwiązania klient VPN musi:* mieć możliwość wyświetlania tekstu powitalnego przy połączeniu do sieci korporacyjnej (tzw. MOTD).
* mieć możliwość sprawdzania, jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.
* być stworzony przez tą samą firmę co dostarczone rozwiązanie.
* ma być dedykowany na platformy: Windows, Linux i MacOS.
* posiadać graficzny interfejs użytkownika, przynajmniej na platformach Windows i MacOS.
* musi posiadać możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN z ukrytymi wszystkimi opcjami konfiguracyjnymi.
* zapewniać obsługę uwierzytelniania wieloskładnikowego
 |
|
|
|
|
|
|
| 43 | Oferowane rozwiązanie musi umożliwiać przydzielanie ustawień tunelu VPN client-to-site na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP. |
| 44 | Oferowane rozwiązanie musi posiadać możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności od atrybutów certyfikatu. |
| 45 | Oferowane rozwiązanie musi zapewniać obsługę uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL. |
| 46 | Oferowane rozwiązanie musi zapewniać możliwość zarządzania pasmem w ramach tunelu VPN i na każdym tunelu VPN z osobna. Rozwiązanie musi automatycznie zmieniać polityki podziału pasma w tunelach VPN po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy. Oferowane rozwiązanie musi zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN. |
| 47 | Oferowane rozwiązanie musi mieć możliwość buforowania danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora. |
| 48 | Oferowane rozwiązanie musi automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN. |
| 49 | Oferowane rozwiązanie musi automatycznie przywracać ostatnią działającą konfigurację sieci po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego. |
| 50 | Oferowane rozwiązanie musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe w przypadku awarii łącza głównego. |
| 51 | Oferowane rozwiązanie musi umożliwiać podział łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping). |
| 52 | Oferowane rozwiązanie musi zapewniać obsługę podziału pasma: dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości). |
|  | 53 | Oferowane rozwiązanie musi posiadać funkcję, która pozwala na zapisywanie całej historii zmian konfiguracji urządzenia. W każdym momencie administrator musi mieć możliwość powrotu do konfiguracji danego modułu z danego dnia oraz informację, jaki użytkownik wprowadził zmianę. Ponadto funkcja musi pozwalać na tworzenie audytów, które pokazują wszystkie zmiany dokonane w konfiguracji wraz z informacją jaki użytkownik je wprowadził. |
|  | 54 | Oferowane rozwiązanie musi wspierać Administrację Urządzeniem opartą na rolach i współdzieleniu pracy kilku administratorów jednocześnie. Kiedy kilku administratorów w jednym momencie konfiguruje różne moduły na firewallu, system musi zapobiegać konfliktom między administratorami oraz logować wszystkie zmiany wprowadzane przez wszystkich administratorów. |
|  | 55 | Oferowane rozwiązanie musi zapewniać dostępną aplikację mobilną umożliwiającą monitoring dostarczonego urządzenia na co najmniej jednym z trzech systemów mobilnych (Windows Mobile/Android/iOS). Aplikacja musi umożliwiać co najmniej:* prezentację ogólnych danych urządzenia (m.in. czas pracy, status licencji, wersja firmware, model i numer seryjny).
* wyświetlanie statusu urządzenia (obciążenie procesora i sieci, zużycia pamięci RAM oraz wykorzystania powierzchni dyskowej a także dane z czujników sprzętowych).
* dynamiczne prezentowanie wykresów dla: przepustowości, ilości sesji dozwolonych i zablokowanych
* wykonanie restartu urządzenia, restartu usług,
* używanie pełnego dostępu terminalowego (SSH).
* włączanie i wyłączanie dynamicznych reguł zapory (na przykład w celu zapewnienia zespołowi tymczasowego dostępu do zablokowanych aplikacji internetowych).

 |
|  |
|  |
|  |
|  |
|  |
|  |
|  | 56 | Oferowane rozwiązanie musi posiadać co najmniej 4 interfejsy sieciowe RJ45 (10/100/1000 MBit). | ………………………………………………………………./wskazać ilość oferowanych interfejsów/ |
|  | 57 | Oferowane rozwiązanie musi posiadać co najmniej 2 GB pamięci operacyjnej RAM. | ………………………………………………………………./wskazać wielkość oferowanej pamięci/ |
|  | 58 | Oferowane rozwiązanie musi posiadać dysk o pojemności co najmniej 30 GB, w technologii SSD. | ………………………………………………………………./wskazać wielkość oferowanego dysku/ |
|  | 59 | Oferowane rozwiązanie musi posiadać minimum 2 złącza USB 2.0 | ………………………………………………………………. /wskazać ilość oferowanych portów USB/ |
|  | 60 | Rozwiązanie musi zapewniać przepustowość firewalla na poziomie minimum 1,35 Gbps.Rozwiązanie musi zapewniać przepustowość silnika IPS na poziomie minimum 500 Mbps.Rozwiązanie musi zapewniać przepustowość dla tuneli VPN na poziomie minimum 240 Mbps.Rozwiązanie musi obsługiwać minimum 80.000 sesji równoległych.Rozwiązanie powinno obsługiwać min 8.000 nowych sesji na sekundę |
|  | 61 | Oferowane rozwiązanie powinno posiadać aktywną wentylację oraz móc pracować w temperaturze dopuszczalnej co najmniej 35 °C | ………………………………………………………………./wskazać dopuszczalną temperaturę pracy/ |
|  | 62 | Oferowane rozwiązanie musi mieć możliwość instalacji w szafie rack (możliwość zamówienia oryginalnych szyn montażowych producenta), a jego wysokość nie może przekraczać 1U |
|  | 63 | Oferowanie rozwiązanie musi zostać dostarczone wraz z trzyletnią subskrypcją na aktualizację poniższych komponentów. |  |
|  | ·         sygnatury antymalware | ………………………………………………………………./wskazać oferowany okres subskrypcji/ |
|  | ·         definicje ataku dla silnika IPS |  |
|  | ·         dostęp do serwerów RBL |  |
|  | 64 | Oferowane rozwiązanie musi posiadać możliwość odpłatnego przedłużenia okresu gwarancji obejmującego wszystkie elementy urządzenia o minimum trzy kolejne lata po wygaśnięciu gwarancji.  |
|  | 65 | W czasie trwania gwarancji Zamawiający musi mieć prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade). |
|  | 66 | W czasie trwania gwarancji zamawiający musi mieć dostęp do wsparcia technicznego producenta świadczonego w systemie 24 godziny/dobę 7 dni w tygodniu (np. w postaci infolinii bądź innego środka porozumiewania się na odległosć/ wymagana jest komunikacja w języku polskim lub angielskim - należy wskazać w ofercie) | ………………………………………………………………./podać numer telefonu wsparcia producenta/ |
|  | 67 | Oferowane rozwiązanie musi posiadać minimum 3 letnią gwarancję obejmującą wszystkie elementy urządzenia włącznie z usługą gwarantującą, że w przypadku awarii sprzętu Zamawiający otrzyma nowe urządzenie w następnym dniu roboczym. | ………………………………………………………………./wskazać oferowany okres gwarancji/ |
|  | 68 | Wykonawca dostarczy dodatkową licencję ochrony przed atakami dnia zerowego (ATD) dla jednego urządzania (w centrali Zamawiającego). | ………………………………………………………………./podać: Tak/Nie/  |
|  | 69 | Wykonawca w ramach realizacji Zamówienia zaoferuje usługę centralnego zarządzania, dostępną dla Zamawiającego w formie usługi chmurowej, na okres minimum 36 miesięcy dla wszystkich oferowanych Firewalli bez dodatkowych opłat po stronie Wykonawcy. | ………………………………………………………………./podać: Tak/Nie/  |
|  | 70 | Oferowane rozwiązanie musi być fabrycznie nowy i nieużywany oraz dostarczony poprzez autoryzowany kanał dystrybucyjny **producenta na terenie Polski.** |