Załącznik nr 1

Zielona Góra, 15.02.2021 r.

Nasz znak: WAF.212.07.2021

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Informacje ogólne

1. Przedmiotem zamówienia jest: **Zakup i dostawa sprzętu sieciowego z oprogramowaniem antywirusowym**
    1. **Przełącznik sieciowy KOD CPV 48219500-1 – 1 sztuka**
    2. **Przełącznik sieciowy KOD CPV 48219500-1 – 2 sztuki**
    3. **ROUTER KOD CPV 48219500-1 – 1 sztuka**
    4. **Oprogramowanie antywirusowe KOD CPV 48761000-0.**
    5. **Wsparcie dla istniejących punktów dostępowych KOD CPV 48219500-1 – 2 sztuka**

II. Miejsce i termin złożenia ofert

1. Ofertę należy złożyć w zamkniętej kopercie osobiście lub listownie do siedziby WFOŚiGW w Zielonej Górze, ul. Miodowa 11, 65-602 Zielona Góra, sekretariat II piętro Funduszu lub przesłać w formie faxu pod nr 68 454 82 52 lub e-mailem na adres: sekretriat@wfosigw.zgora.pl.
2. **do dnia 24.02.2021 r. do godz. 14:00.**

III. Termin realizacji i dostarczenia przedmiotu zamówienia

Do 10 marca 2021 r.

IV. Wymagania dotyczące Wykonawcy

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki:

1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
2) posiadają niezbędną wiedzę i doświadczenie,
3) dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,
4) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

V. Obowiązki Wykonawcy

Do obowiązków Wykonawcy będzie należało:

a) wykonanie przedmiotu zamówienia zgodnie z zasadami współczesnej wiedzy technicznej, obowiązującymi w tym zakresie przepisami i normami technicznymi,

VI. Szczegółowy opis zakupywanego sprzętu

1) **Przełącznik sieciowy KOD 48219500-1 – 1 sztuka**

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa, w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania ".

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Wbudowany redundantny zasilacz.
- Budżet mocy dla portów PoE min.: 250 W.

Maksymalny pobór mocy bez budżetu dla PoE: 35 W.

- Minimalny zakres temperatury pracy: 0-45°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE RJ-45.

- W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

b) 24 porty 1/2.5 GE RJ-45.

c) 24 porty 1/2.5/5 GE RJ-45.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 128 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 204 Mpps.
- Tablica adresów MAC o pojemności co najmniej 16 k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
- Wsparcie dla Private VLAN.
- Obsługa routingu statycznego.
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Centralne zarządzanie sieciami VLAN.
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
   - W przypadku gdy do uruchomienia w/w funkcji wymagane są licencje, producent zobowiązany jest je dostarczyć .
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
- Routing statyczny i dynamiczny (co najmniej OSPF).
- Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2) Przełącznik sieciowy KOD 48219500-1 - 2 sztuki

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa, w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania ".

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Wbudowany redundantny zasilacz.
- Maksymalny pobór mocy: 50 W.
- Minimalny zakres temperatury pracy: 0-50°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.
b) 48 porty 1/2.5 GE RJ-45.
c) 48 porty 1/2.5/5 GE RJ-45.
e) 4 porty 10 GE SFP+.

Zarządzanie

- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32 k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.

- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
- Wsparcie dla Private VLAN.
- Obsługa routingu statycznego.
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedzkowanego VLANu dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Centralne zarządzanie sieciami VLAN.
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
   - Przenoszenie zidentyfikowanych urządzeń do właściwych sterf. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do sterfy odizolowanej.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
   - W przypadku gdy do uruchomienia w/w funkcji wymagane są licencje, producent zobowiązany jest je dostarczyć .
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
- Routing statyczny i dynamiczny (co najmniej OSPF).
- Policy Based Routing.

Gwarancja oraz wsparcie

2. System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

3) ROUTER KOD 48219500-1 – 1 sztuka

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tyś. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6.5 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać 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 musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować 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).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Zielonej Górze,
65-602 Zielona Góra, ul. Miodowa 11, www.wfosigw.zgora.pl

- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać 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 musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać 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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć 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

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Zielonej Górze.
65-602 Zielona Góra, ul. Miodowa 11, www.wfosigw.zgora.pl

bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 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.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4) Oprogramowanie antywirusowe KOD 48761000-0

Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu.

Przedmiotem postępowania jest rozbudowa istniejącego systemu bezpieczeństwa infrastruktury teleinformatycznej o elementy zabezpieczeń dla stacji roboczych wraz z mechanizmami centralnego zarządzania.
Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania.

W ramach postepowania wymaganym jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.
Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

Parametry systemu ochrony dla stacji roboczych.

1. Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy:
    - Kontrola antywirusowa.
    - Funkcja analizy plików w zewnętrznym systemie Sandbox.
    - Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy.
    - URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
    - Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny.
    - Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Zielonej Górze,
65-602 Zielona Góra, ul. Miodowa 11, www.wfosigw.zgora.pl

- Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
- Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
- Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
- Mechanizmy uwierzytelniania dwuskładnikowego
- AntiExploit,
- blokowanie dysków przenośnych typu USB,

2. Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit),Windows Serwer 2019, Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze.

Parametry systemu centralnego zarządzania.

1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.

2. System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox.

3. Ponadto wymagane jest aby system zapewniał:

- integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD,
- definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,
- zautomatyzowany proces zarządzania aplikacja kliencką,
- przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności.
- możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Zielonej Górze,
65-002 Zielona Góra, ul. Miodowa 11, www.wfosigw.zgora.pl

- panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,
- panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych,
- możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych,
- automatyczne wykrywanie stacji klienckich w grupach roboczych,
- logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,
- generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.
- definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,
- zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,
- automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji,
- możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi,
- możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
- możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.

4. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.
5. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

Licencje oraz serwisy.

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:

1. Zainstalowania i centralnego zarządzania 35 aplikacjami klienckimi na stacjach roboczych.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:
   a) Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access,Threat Outbreak Detection, Centralne zarządzanie na okres 60 miesięcy.

3. System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

5) Wsparcie dla istniejących punktów dostępowych KOD CPV 48219500-1 – 2 sztuki

Przedmiotem postępowania jest zapewnienie wsparcia serwisowego oraz aktualizacji oprogramowania dla posiadanych przez Zamawiającego urządzeń dostępowych FortiAP 221C na maksymalny okres przewidziany przez producenta .

Tryb wsparcia technicznego – 24x7.

VII. Kryterium oceny ofert

Cena – 100%

Za najkorzystniejszą zostanie uznana oferta, która ma najniższą cenę, jeżeli wybór oferty najkorzystniejszej będzie niemożliwy z uwagi na to, że dwie lub więcej ofert posiada taką samą cenę, zamawiający wezwie wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych.

Zamawiający nie dopuszcza możliwości składania ofert wariantowych oraz ofert częściowych przez Wykonawców.

VIII. Kontakt

1. Osobą do kontaktów ze strony WFOŚiGW w Zielonej Górze jest Andrzej Jodajtis tel. 68 419 69 16, email: ajodajtis@wfosigw.zgora.pl.
2. Zamawiający udziela odpowiedzi wszystkim wykonawcom, jak i zapewnia dostęp do wszystkich posiadanych dokumentów dotyczących przedmiotu zamówienia, w godzinach pracy Funduszu, w dni robocze, w godzinach od godz. 8:30 do godz. 15:00.

IX. Czas związania ofertą

1. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca pozostaje związany ofertą przez okres 14 dni od upływu daty składania ofert.

X. Postanowienia końcowe

1. Zamawiający nie ponosi żadnych kosztów związanych z przejazdem, dostawą, ubezpieczeniem w trakcie transportu, zakwaterowaniem i wyżywieniem wykonawcy.
2. Zamawiający zastrzega sobie prawo do zamknięcia postępowania (nierozstrzygnięcia), bez podania przyczyn.

15 -02- 2021 Juliusz Kordoń
(ES ds. zamówień publicznych)

Prezes Zarządu
15 -02- 2021 Mariusz Herbut
(podpis zatwierdzającego Prezesa Zarządu)

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Zielonej Górze,
65-602 Zielona Góra, ul. Miodowa 11, www.wfosigw.zgora.pl