WOJEWÓDZKI FUNDUSZ OCHRONY ŚRODOWISKA I GOSPODARKI WODNEJ W KIELCACH
al.ks.Jerzego Popiełuszki 41, 25-155 Kielce
tel. sekretariat 41 366 15 12, 41 333 52 20
tel. biuro obsługi 41 368 02 13, 41333 52 21
fax 41 366 09 05
http://www.wfos.com.pl, email: biuro@wfos.com.pl

Zał. nr 1 do zaproszenia

DAI 0104-16/20

OPIS PRZEDMIOTU ZAMÓWIENIA

Urządzenia komputerowe wraz z peryferiami i oprogramowaniem

PREZES ZARZĄDU
Ryszard Gliwiński

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

WOJEWÓDZKI FUNDUSZ OCHRONY ŚRODOWISKA I GOSPODARKI WODNEJ W KIELCACH
al.ks.Jerzego Popiełuszki 41, 25-155 Kielce
tel. sekretariat 41 366 15 12, 41 333 52 20
tel. biuro obsługi 41 368 02 13, 41333 52 21
fax 41 366 09 05
http://www.wfos.com.pl, email: biuro@wfos.com.pl

Część I

1. Komputer typu Laptop – 11 szt.

Komputery typu Laptop muszą być identyczne (ten sam producent, model i konfiguracja sprzętowa). Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Komputer musi spełniać poniższe minimalne wymagania:

Lp.	Opis Elementów	Wymagania minimalne
1	Ekran	• wymiary: min. 15.0 cala max.16,0 cala, • typ matrycy: **matowa** (przeciwodblaskowa/Anti-Glare), • rozdzielczość: min. 1920 x 1080,
2	Procesor	• 64 bit -o wydajności min. **6 300** punktów w teście Passmark CPU Mark dostępnym na stronie https://www.cpubenchmark.net/cpu_list.php
3	Pamięć RAM	• min. **16 GB RAM,** **ZAMAWIAJĄCY dopuszcza składanie ofert w których dostarczony sprzęt będzie posiadał fabrycznie zainstalowane 8GB pamięci RAM.** **WYKONAWCA jest zobowiązany dostarczyć lub samodzielnie zainstalować dodatkową kość pamięci RAM tak aby spełnić minimalne wymagania ZAMAWIAJĄCEGO w zakresie komputera typu Laptop. Dodatkowa kość pamięci RAM musi być w 100% kompatybilna z dostarczonym sprzętem.** **WYKONAWCA jest zobowiązany oświadczyć że integracja w hardware urządzenia (m.in. dołożenie dodatkowej kości pamięci – zgodnie ze sztuką) nie wpłynie w żaden sposób na okres gwarancji producenta dostarczonego sprzętu.**
4	porty, interfejsy, komunikacja	• min. 1 port USB Typu-C, • min. 2 porty USB 3.0 lub nowsze • min. 1 port HDMI lub DisplayPort, • min. 1 czytnik kart pamięci, • wbudowana karta sieciowa Ethernet, • wbudowana karta bezprzewodowa standard min. IEEE 802.11ac, • Bluetooth, • kamera internetowa min. HD • złącze stacji dokującej, alternatywnie wykorzystując istniejący port USB typu C ww. złącze lub port musi umożliwić podłączenie stacji dokującej opisanej w pkt 3 (Stacja dokująca)
5	Dysk	• dysk SSD M.2, o pojemności min. **500 GB**
6	Zabezpieczenia	• sprzętowy układ szyfrowania lub inny równoważny, zapewniający szyfrowanie dysku,
7	Układ graficzny	• wbudowany lub dedykowany min. **UHD**

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

8	Przewody i peryferia	• komplet przewodów przewidziany przez producenta urządzenia • bezprzewodowy zestaw klawiatura + mysz o minimalnych parametrach: o Pełnowymiarowa klawiatura z klawiaturą numeryczną, klawiszami strzałek i dziewięcioma klawiszami funkcyjnym (numerami). o odbiornik o wielkości sklasyfikowanej jako: Nanoodbiornik o 2 baterie AAA do klawiatury i 1 bateria AA do myszy o możliwość umieszczenia nanoodbiornika pod pokrywą myszy (np. tuż obok baterii) w specjalnie przygotowanym dla niego miejscu. Pokrywa myszy po włożeniu nanoodbiornika musi umożliwić bezproblemowe zamknięcie. o gwarancja 36 miesięcy • podkładka pod mysz z żelową podpórką pod nadgarstek, który unosi nadgarstek zapewniając ergonomiczne ułożenie dłoni. • podkładka powinna zapewnić płynną pracę myszom optycznym. • podkładka powinna posiadać antypoślizgowy spód, który zapewnia stabilność pracy. • Torba na sprzęt
9	Gwarancja	• **gwarancja min. 36 miesięcy (on-site alternatywnie door-to-door),** • możliwość pobierania dokumentacji i sterowników z sieci Internet (portali producenta), • możliwość uzyskania pomocy technicznej producenta w języku polskim, • serwis realizowany w języku polskim, • **w przypadku uszkodzenia dysku, wymiana na nowy z pozostawieniem uszkodzonego.**
10	Certyfikaty	• certyfikat CE,
11	System operacyjny	• zainstalowany system operacyjny w polskiej wersji językowej, 64 bitowy: o kompatybilny i obsługujący Active Directory (usługę katalogową) wykorzystywaną przez zamawiającego o wbudowana funkcja systemowa umożliwiająca zarządzanie wirtualnymi maszynami (hypervisor), o wbudowaną funkcję szyfrowania dysków, o wbudowana funkcja tworzenia obrazu systemu, o DODATKOWO POWINIEN POSIADAĆ: ▪ firewall systemowy, ▪ systemowa funkcja przywracania systemu, ▪ wbudowane oprogramowanie chroniące przed programami szpiegującymi, ▪ zgodność z najnowszym oprogramowaniem biurowym funkcjonującym na rynku polskim, ▪ wyszukiwarka plików, ▪ obsługa pulpitu zdalnego, ▪ kopia zapasowa w tle, ▪ interfejs w języku polskim,

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		▪ system 64 bitowy, ▪ obsługa sieci firmowych ▪ obsługa historii plików, ▪ Obsługa automatycznych aktualizacji systemowych ▪ obsługa wirtualnych pulpitów

2. Monitor LCD – 11 szt.

Monitory muszą być identyczne (ten sam producent, model i konfiguracja sprzętowa). Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Monitor musi spełniać poniższe wymagania:

Lp.	Opis elementów	Minimalne wymagania
1	Parametry	• przekątna ekranu(cale): min. 23 max. 25 • rozdzielczość **min. 1920x1080** • proporcje ekranu 16:9 • typ matrycy: **matowa** (przeciwodblaskowa/Anti-Glare), • redukcja niebieskiego światła • wbudowane głośniki
2	Złącza	• min. 1szt. HDMI lub DisplayPort ***(Wykonawca dostarczy odpowiednie okablowanie/przejściówki do podłączenia zaproponowanego monitora z zaproponowaną stacją dokującą – opisaną w pkt 3)*** • min. 2 szt. port USB typ 3.0 lub nowszy
3	Dodatkowe informacje	• **podstawa umożliwiająca regulację ekranu:** **- góra, dół** **- kąt nachylenia.**
4	Przewody	Komplet przewodów przewidziany przez producenta
5	Certyfikat	Certyfikat CE
6	Gwarancja	**36 `miesięcy**

3. Stacja dokująca/ Dock – 11 szt.

Stacje dokujące muszą być identyczne (ten sam producent, model). Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zaoferowana stacja dokująca lub dock musi być tego samego producenta co zaoferowany sprzęt (Komputer typu Laptop), musi być kompatybilna z zaoferowanym laptopem w 100%. Stacja dokująca musi spełniać poniższe wymagania:

Lp	Opis elementów	Minimalne wymagania
1	Stacja dokująca lub dock	Interfejsy: • min 3 szt. USB 3.0 lub nowszy

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• min. 1 HDMI lub DisplayPort lub oba porty (Wykonawca dostarczy odpowiednie okablowanie do podłączenia stacji dokującej z zaoferowanym monitorem – co najmniej 3 metrowy) • min 1. Port RJ-45 Gigabit Ethernet , • Złącze zasilania • **gwarancja min. 36 miesiące (on-site alternatywnie door-to-door),**
2.	Inne	Stacja dokująca/dock prócz replikacji portów ma za zadanie dostarczyć ładowanie do podłączonego urządzenia – tak aby nie trzeba było korzystać z zasilacza laptopa.

4. Pakiet oprogramowania biurowego -11 szt.

Przedmiot dotyczy dostawy nowych 11 szt. licencji oprogramowania biurowego o min. 12 miesięcznym okresie ważności każdej z licencji. Zaproponowany pakiet biurowy musi być w 100% kompatybilny z już posiadanymi licencjami pakietu Microsoft 365 Business Standard

Zaproponowany pakiet musi zawierać min.:

- edytor tekstu - wersja chmurowa zgodna z przepisami RODO oraz offline (możliwość instalacji np. na systemie operacyjnym Windows),
- arkusz kalkulacyjny - wersja chmurowa zgodna z przepisami RODO oraz offline (możliwość instalacji np. na systemie operacyjnym Windows),
- program do przygotowywania i prowadzenia prezentacji - wersja chmurowa zgodna z przepisami RODO oraz offline (możliwość instalacji np. na systemie operacyjnym Windows),
- aplikacja do obsługi relacyjnych baz danych,
- program do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami - chmurowa zgodna z przepisami RODO oraz offline (możliwość instalacji np. na systemie operacyjnym Windows);
- program/aplikacja chmurowa zgodna z przepisami RODO do prowadzenia spotkań/wideo rozmów z wcześniej zaproszonymi użytkownikami tej samej organizacji lub gośćmi (spoza organizacji)
- min. 1 TB przestrzeni dyskowej dostępnej w bezpiecznej chmurze do przechowywania i udostępniania plików do i poza organizację,

1) Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą;
2) Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej pomocy technicznej;
3) Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, w tym obsługa formatowania bez utraty parametrów i cech użytkowych
4) Wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł
5) Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF;

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

6) Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich elementów;
7) Możliwość jednoczesnej pracy wielu użytkowników na udostępnionym dokumencie arkusza kalkulacyjnego;
8) Posiadać pełną kompatybilność z systemami operacyjnymi:
   - MS Windows 10 (32 i 64-bit).

Część II

5. NAS - urządzenie do kopii zapasowych

Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. NAS musi spełniać poniższe minimalne wymagania:

Lp.	Opis Elementów	Wymagania minimalne
1	Procesor	• architektura procesora : 64-bit • min. 6 rdzeń, • częstotliwość procesora min. 2,1 GHz • wbudowany mechanizm szyfrowania sprzętowego
2	Pamięć RAM	• min 32 GB DDR4 (parametry: 2x16GB) • gniazd pamięci min. 4 • możliwość rozszerzenia pamięci RAM do min. 64GB • zainstalowane pamięci RAM muszą być w 100% kompatybilne z oferowanym sprzętem
3.	Przechowywanie	• wbudowane kieszenie na dyski min. 12 szt. • możliwość zastosowania dedykowanych przez producenta sprzętu modułów rozszerzających ilość kieszeni dysków do min. 24 szt.
4	Zgodność dysków	• 3.5" SATA HDD • 2.5" SATA HDD • 2.5" SATA SSD
5	Porty zewnętrzne	• min. 4 szt. port LAN RJ-45 1GbE (z obsługą funkcji Link Aggregation) • min. 2 szt. port LAN RJ-45 10GbE (z obsługą funkcji Link Aggregation) • min 2 szt. USB.3.0 lub nowsze
6	PCIe	• min. 2 szt. kart rozszerzeń PCIe Gen3
7	System plików	• EXT4 • EXT3 • FAT • NTFS
8	Obudowa	• Obudowa typu RACK
9	Inne	• Dysk z możliwością wymiany podczas pracy (hot-swap)
10	Dyski/ rozwiązanie RAID	**Urządzenie powinno umożliwiać utworzenie co najmniej dwóch niezależnych grup RAID** • **WYKONAWCA dostarczy wraz z urządzeniem** ○ **4 szt. dysków SSD o pojemności min. 3,84 TB każdy**

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		W celu utworzenia grupy RAID 5 ○ **7 szt. dysków HDD o pojemności min. 4 TB każdy** **W celu utworzenia grupy RAID 6** Wszystkie dostarczone dyski (SSD, HDD) muszą być w **100% kompatybilne z proponowanym urządzeniem.** Co WYKONAWCA potwierdzi u producenta dostarczonego urządzenia. Zaoferowane dyski SSD muszą być klasy Enterprise/korporacyjnej przystosowane do pracy ciągłej 24/7. Minimalne parametry dysków HDD: • dostosowane do pracy ciągłej 24/7, • prędkość obrotowa min. 7200 • pamięć cache min. 256 MB • klasy Enterprise/Data Center
11	System operacyjny/ obsługa funkcjonalności	System operacyjny/ zarządzania umożliwiający tworzenie i zarządzanie opcjami systemowymi w interfejsie graficznym. Dostęp do systemu np. przez przeglądarkę Umożliwiający konfigurowanie: • Min. liczba wolumenów wewnętrznych: 200 • Min. liczba celów iSCSI: 200 • Obsługiwane typy macierzy RAID ○ RAID 1 ○ RAID 5 ○ RAID 6 ○ RAID 10 • Migracja macierzy RAID ○ Basic to RAID 1 ○ Basic to RAID 5 ○ RAID 1 to RAID 5 ○ RAID 5 to RAID 6 • Powiększenie wolumenu za pomocą większych dysków twardych ○ RAID 1 ○ RAID 5 ○ RAID 6 ○ RAID 10 • Powiększenie wolumenu przez dodanie dysków twardych ○ RAID 5 ○ RAID 6 • Typy macierzy RAID obsługujące Hot Spare ○ RAID 1 ○ RAID 5 ○ RAID 6 ○ RAID 10 • Integracja listy kontroli dostępu systemu Windows (ACL) • centrum logów/zdarzeń, • Protokoły sieciowe: ○ SMB, ○ NFS, ○ SSH, ○ iSCSI, ○ HTTP, ○ HTTPs,

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		○ FTP, ○ SNMP, ○ LDAP.
12	Kopia zapasowa	W pełni **darmowe oraz zintegrowane** oprogramowanie do tworzenia kopii zapasowych i przywracania danych. Oprogramowanie musi umożliwić tworzenie kopii zapasowych nieograniczonej liczby punktów końcowych Windows oraz maszyn wirtualnych (Hyper-V) bez dodatkowych kosztów licencji na oprogramowanie. • Oprogramowanie ma umożliwić różne metody przywracania, w tym przywracanie całego urządzenia, szczegółowe odzyskiwanie plików, • tworzenie kopii zapasowych typu: ○ bare-metal (BMR) obraz dysków ○ przyrostowe • tworzenie harmonogramów tworzenia kopii zapasowych w centralnym punkcie zarządzania kopiami zapasowymi, • centralny interfejs graficzny zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, • wykorzystanie technologii deduplikacji podczas tworzenia kopii zapasowych • wsparcie i aktualizacje dla oprogramowania kopii zapasowych bezterminowe
13	Gwarancja	• min. 5 lat na urządzenie • min. 5 lat na dysk HDD (**w przypadku uszkodzenia dysku, wymiana na nowy z pozostawieniem uszkodzonego.**) • min. 5 lat na dysk SSD (**w przypadku uszkodzenia dysku, wymiana na nowy z pozostawieniem uszkodzonego.**)
14	Pomoc techniczna	• pomoc techniczna/support świadczona przez producenta sprzętu lub WYKONAWCĘ (sprzedawcę) w języku polskim • WYKONAWCA zapewni wsparcie posprzedażowe przez inżyniera w czasie trwania gwarancji
15	Szkolenie	• WYKONAWCA zobowiązany jest przeszkolić Pracowników działu IT ZAMAWIAJĄCEGO z rozwiązania, które dostarczy. Szkolenie nie może być krótsze jak 8 godzin, (max. Ilość godzin jaką ZAMAWIAJCY jest w stanie dziennie poświęcić na szkolenie to 4 h. Prowadzący szkolenie dokona konfiguracji i dostosowania dostarczonego urządzenia wraz z pracownikami działu IT. Szkolenie zorganizowane w formie online, w szkoleniu będzie brało udział dwóch Pracowników działu IT ZAMAWIAJĄCEGO. Termin szkolenia będzie ustalony po dostarczeniu rozwiązania i jego wdrożeniu. Szkolenie musi zostać przeprowadzone przez inżyniera, który ma doświadczenie w prowadzeniu tego typu szkoleń.
16	Inne	• **szafa instalacyjna RACK** 19" wisząca w kolorze jasnym z częściowym szklanym frontem,

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• **wymiary zew. [mm] szer. gł.: 600x600,** • wysokość 15U akcesoria dodatkowe: o 2 szt. wentylator serwerowy o 1. szt. termostat o organizer kabli 1U poziomy, o 1 szt. listwa zasilająca RACK 19" ▪ liczba gniazd: min 8x, ▪ wysokość robocza: 1U,

Część III

6. UTM – urządzenie zabezpieczające sieć

Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta.
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.

Lp.	Opis Elementów	Wymagania minimalne
1	System musi wspierać IPv4 oraz IPv6 w zakresie:	• Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego
	Redundancja, monitoring i wykrywanie awarii	• 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. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• Monitoring stanu realizowanych połączeń VPN. • System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych
	Interfejsy, Dysk, Zasilanie:	• System realizujący funkcję Firewall musi dysponować minimum: o 10 portami Gigabit Ethernet RJ-45. • System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. • W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System musi być wyposażony w zasilanie AC. • **Wbudowany dysk twardy m.in. do przechowywania logów**
	Parametry wydajnościowe:	• W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. • Przepustowość Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 6.2 Gbps. • 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 1.4 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https minimum 720 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: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• Analiza ruchu szyfrowanego protokołem SSL.
	Polityki, Firewall	• Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: o Translację jeden do jeden oraz jeden do wielu. o Dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
	Połączenia VPN	• System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: o Wsparcie dla IKE v1 oraz v2. o Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). o Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. o Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. o Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. o Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. o Mechanizm „Split tunneling" dla połączeń Client-to-Site. • System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: o 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. o Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. o **Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.**
	Routing i obsługa łączy WAN	• W zakresie routingu rozwiązanie powinno zapewniać obsługę: o Routingu statycznego. o Policy Based Routingu. o Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	Zarządzanie pasmem	• System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. • System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
	Ochrona przed malware	• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. • System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
	Ochrona przed atakami	• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • 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. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
	Kontrola aplikacji	• Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
	Kontrola WWW	• Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• 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. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google czy Yahoo. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. • 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	• System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: o Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. o Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. o Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. • Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
	Zarządzanie	• 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. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping,

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • 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	• 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. • 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. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
	Zabezpieczenie końcówek PC (Endpoint Protection)	• Dedykowane oprogramowanie producenta sprzętu, instalowane na urządzeniach końcowych np. komputerach stacjonarnych/laptopach z systemem operacyjnym Win 10 lub 8.1. tzn. „agent", który posiada min.: o Ochrona przed AntiMalware o Web Filtering o Kontrola urządzeń USB o Inwentaryzacja oprogramowania o Połączenia zdalne ▪ IPSec VPN ▪ SSL VPN o Centralne zarządzanie o Centralne miejsce na logi i raporty Licencja dla min. 60 końcówek (komputerów, laptopów) Na okres **12 miesięcy**
	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: • Firewall, • 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

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• Urządzenie w ramach dostarczonych licencji musi mieć możliwość bezpiecznego udostępnienia aplikacji webowych (stron internetowych) w sieci WAN – zabezpieczenie typu WAF. • Centralne zarządzanie oraz analiza logami bezpośrednio na urządzeniu i w chmurze o czas przechowywania logów co najmniej 12 miesięcy licencje na okres **36 miesięcy**.
	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres **36 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.** W przypadku uszkodzenia sprzętu wymiana na nowe – maksymalny czas dostawy nowego urządzenia do siedziby ZAMAWIJACEGO nie może być dłuższy niż **4 godz.** Ponadto WYKONAWCA zapewni: • Wsparcie techniczne certyfikowanych inżynierów, • Pomoc przy rejestracji urządzenia, • Doradztwo w zakresie konfiguracji, • Zakładanie zgłoszeń serwisowych u Producenta rozwiązania, • Pomoc w procesie realizacji naprawy i wymiany urządzeń w ramach gwarancji urządzenia, • **Wdrożenie urządzenia zgodnie z instrukcjami i pod potrzeby ZAMAWIAJĄCEGO (pełna konfiguracja)** • w przypadku konieczności zmiany konfiguracji urządzenia – pomoc w dostosowaniu do aktualnych potrzeb (min. 15 zgłoszeń na rok).
	Szkolenie	**WYKONAWCA zobowiązany jest przeszkolić Pracowników działu IT ZAMAWIAJĄCEGO z rozwiązania, które dostarczy.** Szkolenie ma zostać przygotowane i przeprowadzone w pełni profesjonalnie, WYKONAWCA, w ramach składanej oferty dostarczy agendę szkolenia wraz z potrzebnym czasem jaki będzie potrzebny na przepracowanie danych zagadnień. Przed szkoleniem ZAMAWIAJĄCY zobowiązany jest dostarczyć materiały szkoleniowe, zgodne z agendą szkolenia. Na szkoleniu powinna być przedstawiona praktyczna wiedza połączona z przykładami oraz ćwiczeniami dla kursantów w postaci laboratoriów. Szkolenie ma objąć zagadnienia **podstawowe jak również średnio zaawansowane dostarczonego rozwiązania** m.in. takie jak (*ZAMAWIAJĄCY nie określa tutaj wszystkich zagadnień, które WYKONAWCA przeprowadzi w ramach swojego autorskiego szkolenia, a jedynie te, które muszą być*) kursant po szkoleniu będzie miał wiedzę z zakresu:

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

		• podstawowych zagadnień związanych z szyfrowaniem oraz operacje oparte na certyfikatach. • potrafił identyfikować ruch zabezpieczony protokołem SSL/TLS, i przeciwdziałać ewentualnemu obchodzeniu reguł bezpieczeństwa poprzez szyfrowanie komunikacji. • stosować techniki kontroli aplikacji do monitorowania i kontrolowania komunikacji sieciowej, które mogą wykorzystywać standardowe lub niestandardowe protokoły i porty. • chronić się przed wyciekami danych, identyfikując pliki z danymi wrażliwymi i blokując możliwość ich przesłania poza chronione sieci. • zbierać i prawidłowo interpretować logi. • umiejętnie walcz z podstawowymi technikami hackerskimi i zabezpieczyć się przed atakami • Analizować ruch sieciowy na urządzeniu, wykrywać i podejmować decyzję nt. utworzenia odpowiednich ról na firewall w celu zablokowania lub przepuszczenia danego ruchu. Szkolenie nie może być krótsze jak **20 godzin**, (**max. Ilość godzin jaką ZAMAWIAJĄCY** jest w stanie **dziennie poświęcić na szkolenie to 4 h.** Szkolenie zorganizowane w formie **online**, w szkoleniu będzie brało udział dwóch Pracowników działu IT ZAMAWIAJĄCEGO. Termin szkolenia będzie ustalony po dostarczeniu rozwiązania i jego wdrożeniu. Szkolenie musi zostać przeprowadzone przez **certyfikowanego inżyniera, który posiada najwyższy stopień certyfikacji danego rozwiązania oraz ma doświadczenie w prowadzeniu tego typu szkoleń.**
	Wdrożenie	WYKONAWCA po dostarczeniu rozwiązania, w ramach oferty wdroży ww. system. Wdrożenie obejmuje min.: • konfiguracja metod logowania, • konfiguracja Interface, • konfiguracja podsieci, • Konfiguracja DMZ, • konfiguracja WAN, SD-WAN, routing • konfiguracja polityk bezpieczeństwa (zgodnych z zapotrzebowaniem) • konfiguracja profili bezpieczeństwa (zgodnych z zapotrzebowaniem) • stworzenie obiektów zgodnych z topologią sieci • konfiguracja przekierowań • konfiguracja VPN Client-2-Site • konfiguracja VPN Site-2-Site • konfiguracja ustawień systemowych urządzenia • testowanie wdrożonej konfiguracji • utworzenie kopi zapasowej po zakończonej pracy • inne konfiguracje, które podczas wdrożenia zleci ZAMAWIAJĄCY

Paweł Nowak
Specjalista w Wieloosobowym stanowisku
ds. technologii informacyjnej

PREZES ZARZĄDU
Ryszard Gliwiński