Załącznik 6.1. do SIWZ

SP.ZP.272.49.2018.II.FR

Opis Przedmiotu Zamówienia

Zadanie 1 – Dostawa i wdrożenie infrastruktury sieciowej – aktywnej i pasywnej dla Powiatu Wrocławskiego

Zamówienie realizowane w ramach projektu pn**.** „Zwiększenie dostępności i jakości elektronicznych usług publicznych dla mieszkańców i podmiotów gospodarczych Powiatu Wrocławskiego oraz 8 Gmin: Czernicy, Długołęki, Jordanowa Śląskiego, Kątów Wrocławskich, Kobierzyc, Mietkowa, Siechnic i Żórawiny”. współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020; Oś Priorytetowa 2 Technologie Informacyno - Komunikacyjne; Działanie 2.1 E-usługi publiczne, Poddziałanie 2.1.1 E-usługi publiczne – konkurs horyzontalny.

1. Zestawienie zbiorcze sprzętu - Dostawa infrastruktury sieciowej – aktywnej i pasywnej

Dostawa infrastruktury sieciowej – aktywnej i pasywnej		Powiat Wrocławski
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Przełącznik rdzeniowy	3
2.	Przełącznik dostępowy	15
3.	Urządzenie brzegowe UTM	2
4.	Urządzenie do analizy ruchu - sieciowego	1
5.	Rozbudowa sieci dostępowej	2

2. Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia

W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

- Dostawę urządzeń teleinformatycznych w zakresie poz. 1 i 2 powyższej tabeli,
- Dostawę, instalację, konfigurację i uruchomienie poz. 3,4,5 zgodnie ze wskazaniem Zamawiającego urządzenia do analizy ruchu sieciowego, urządzeń dostępowych oraz urządzeń UTM.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia

3.1. Rozbudowa infrastruktury sieciowej/Przełącznik rdzeniowy – 3 szt.

1. Przełącznik warstwy dostępowej z obsługą AP:
2. Przełącznik stackowalny wyposażony w 24 porty 10/100/1000BaseT
3. Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
   a. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP
   b. Minimum 2-portowy moduł 10Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystania pojedynczego łącza 10GE istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP
4. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH)
5. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:
   a. Przepustowość w ramach stosu min. 480Gb/s
   b. Min. 9 urządzeń w stosie
   c. Zarządzanie poprzez jeden adres IP

d. Możliwość tworzenia połączeń z kilku ethernetowych łączy fizycznych w jedno logiczne (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad
e. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE)

6. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
7. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne
8. Przełącznik musi posiadać możliwość rozbudowy o funkcję kontrolera sieci bezprzewodowej WiFi:
   a. Przełącznik musi zapewniać centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) po zainstalowaniu odpowiedniej licencji
   b. Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s
   c. Obsługa minimum 2000 klientów sieci WiFi
   d. Możliwość terminowania tuneli CAPWAP na przełączniku (zapewnienie jednego punktu nakładania polityk QoS/bezpieczeństwa dla sieci LAN/WLAN)
9. Szybkość przełączania minimum 65Mpps dla pakietów 64-bajtowych
10. Minimum 4 GB pamięci DRAM i 2GB pamięci flash
11. Obsługa minimum :
    a. 1.000 sieci VLAN
    b. 32.000 adresów MAC
    c. 24.000 tras routingu
12. Obsługa protokołu NTP
13. Obsługa IGMPv1/2/3
14. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree
    b. IEEE 802.1s Multi-Instance Spanning Tree
15. Obsługa protokołu LLDP i LLDP-MED
16. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
17. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X

g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
h. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
i. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
j. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
k. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)

19. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
b. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi
c. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek
d. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
f. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik
g. Kontrola sztormów dla ruchu broadcast/multicast/unicast
h. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

20. Wbudowane reflektometry (TDR) dla portów 10/100/1000
21. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych
22. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
23. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000 . Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow
24. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
25. Dedykowany port Ethernet do zarządzania out-of-band

26. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
27. Urządzenie musi być wyposażone w port konsoli USB
28. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją
29. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
30. Możliwość montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1 RU
31. Urządzenie ma być dostarczone wraz z 2-portowym modułem 10Gigabit Ethernet SFP+ Multimode (wraz z dwoma wkładkami GBic, kablami do stackowania o długości 0,5m i patchcordami światłowodowymi (długość 5 m) do podłączenia serwerów Zamawiającego wyposażonych w złącze typu LC.

    Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy CISCO. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami CISCO zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.). W zestawie wymagane jest dostarczenie dwóch kabli do stackowania.

    W wypadku dostarczenia innych urządzeń niż urządzenia marki CISCO wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. Ponadto zapewni wdrożenie i konfigurację systemu. A w wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.

3.2. Rozbudowa infrastruktury sieciowej/Przełączniki dostępowe – 15 szt.

1. Typ i liczba portów:
   a. Minimum 24 portów 10/100/1000.
   b. Minimum 4 dodatkowe porty uplink 1 Gigabit Ethernet SFP.
   c. Porty SFP muszą umożliwiać ich obsadzanie wkładkami GigabitEthernet – minimum 1000Base- SX, 1000Base LX/LH, 1000Base-BX-D/U zależnie od potrzeb Zamawiającego.
2. Co najmniej 512MB pamięci DRAM oraz co najmniej 128MB pamięci Flash
3. Wielkość tablicy adresów MAC: co najmniej 16 000 .
4. Ilość obsługiwanych sieci VLAN: co najmniej 1 000
5. Wydajność:
   a. Przepustowość zapewniająca wydajność Line-rate
   b. Przełączanie dla pakietów 64-bajtowych: min. 71.4 Mpps.
6. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości co najmniej 9216 bajtów
7. Funkcjonalność urządzenia
   a. Obsługa co najmniej 16 statycznych tras dla routingu IPv4 i IPv6,
   b. Obsługa protokołu NTP,
   c. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping,
   d. Możliwość uruchomienia funkcjonalności DHCP Server,

e. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree – wymagane wsparcie dla min. 128 instancji protokołu STP,
f. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP),
g. Musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP),
h. Musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB,
i. Musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli,
j. Musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN),
k. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych,
l. Możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
    - do min. 8 jednostek w stosie,
    - magistrala stakująca o przepustowości co najmniej 80Gb/s
    - możliwość tworzenia połączeń z kilku ethernetowych łączy fizycznych w jedno logiczne zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie

8. Bezpieczeństwo
a. Minimum 4 poziomy dostępu administracyjnego poprzez konsolę,
b. Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
c. Obsługa funkcji Guest VLAN,
d. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
e. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
f. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie,
g. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6,
h. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) - zarówno dla IPv4 jak i IPv6,
i. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard,
j. Funkcjonalność Protected Port,
k. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
l. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).

9. Wsparcie dla mechanizmów zapewnienia jakość usług w sieci
a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek,
c. Możliwość obsługi jednej z powyżej wymienionych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
d. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.
e. 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszcza się także rozwiązanie zewnętrzne)

10. Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''
11. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy CISCO. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami CISCO zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.).**

    W wypadku dostarczenia innych urządzeń niż urządzenia marki CISCO wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego Śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. Ponadto zapewni wdrożenie i konfigurację systemu. A w wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.

3.3. Urządzenie brzegowe UTM – 2 szt.

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. Powinna istnieć możliwość dedykowania 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 oraz 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, Dyski:

1. System realizujący funkcję Firewall musi dysponować minimum 20 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps.
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 realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1,8 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,9 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 190 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, IMAP.
- Zarządzanie pasmem (QoS, Traffic shaping).
- Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- 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.

Polityki, Firewall

1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
3. 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.
4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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 Diffiego-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.
    - 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.
3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

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.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

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.

Kontrola Antywirusowa

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. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. 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.

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 2800 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, Botnet.
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, phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: np. Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania 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 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 certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla pakietów obejmujących: Kontrolę aplikacji,IPS, Antywirus, Antyspam, Web Filtering, Sandbox, ochrona systemów mobilnych , upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres min: 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min 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 8x5.

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 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.
3. **Uwaga: Zamawiający posiada 5 access pointów firmy Fortinet które muszą być zarządzane z poziomu UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenia dostępowe na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego Śląska).**

3.4. Urządzenie do analizy ruchu sieciowego – 1 szt.

System centralnego logowania, raportowania i korelacji logów

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej musi ono odpowiadać minimalnym wymaganiom jak dla platformy sprzętowej.

Dostarczone rozwiązanie musi w pełni współpracować z dostarczonymi urządzeniami brzegowymi UTM.

Interfejsy, Dyski:

1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45 (nie dotyczy wersji programowej).
2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB (nie dotyczy wersji programowej).

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 100 GB logów na dzień.

2. System musi być w stanie przeanalizować minimum 3000 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 150 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
    a. Listę najczęściej wykrywanych ataków.
    b. Listę najbardziej aktywnych użytkowników.
    c. Listę najczęściej wykorzystywanych aplikacji.
    d. Listę najczęściej odwiedzanych stron www.
    e. Listę krajów , do których realizowana jest komunikacja.
    f. Listę najczęściej wykorzystywanych polityk Firewall.
    g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów, co najmniej po typie logów (traffic, zdarzeń ataków, wykrycia malware'u, odwiedzanych stron, wykrytych aplikacji sieciowych).
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja Logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii eventów:
    - Malware.
    - Kontroli aplikacji.

- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
    a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać definiowanie co najmniej 2 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 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 8x5.
   Oferent winien przedłożyć dokumenty:
    a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
    b) Certyfikat ISO 9001 podmiotu serwisującego.
2. 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 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.
3. 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.

3.5. Rozbudowa sieci dostępowej wifi – 2 kpl.

Tryb pracy	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
Obudowa	Kompaktowa obudowa z tworzywa sztucznego umożliwiającą montaż na suficie lub ścianie wewnątrz budynku.
Moduł radiowy	Musi być wyposażone w dwa niezależne moduły radiowe pracujące odpowiednio w pasmach: 5 GHz a/n/ac oraz 2,4 GHz b/g/n. Urządzenie musi pozwalać na

	jednoczesne rozgłaszanie co najmniej 14 SSID Przepustowość : • Dla radia 2,4 GHz: 300 Mbps • Dla radia 5 GHz: 867 Mbps Mechanizmy kolejkowania dla różnych klas ruchu: dane, voice, video Mechanizmy ochrony przed atakami na sieć radiową Wymagana moc nadawania min 20 dBm Mechanizmy uwierzytelniania 802.1x, w tym obsługa protokołów EAP: TLS, TTLS/MSCHAPv2, PEAP, GTC, SIM Możliwość tunelowania całej komunikacji do kontrolera sieci bezprzewodowych jak również funkcja bridge'owania ruchu z poszczególnych SSID do VLAN.
Anteny	Minimum 4 wbudowane anteny
Interfejsy	Interfejs sieciowy w standardzie 10/100/1000 Base-TX
Zasilanie	Możliwość zasilania w standardzie PoE 802.3af

W ramach postępowania powinien zostać dostarczony kontroler sieci bezprzewodowych, zarządzający planowaną strukturą urządzeń bezprzewodowych Access Point. Kontroler powinien oferować środowisko graficzne pozwalające na wykrywanie punktów dostępowych podpinanych do sieci a następnie na zarządzanie nimi.

Powinien umożliwiać zarządzanie grupą wskazanych przez Zamawiającego punktów dostępowych z możliwością rozbudowy do wartości docelowej.

4. Wymagania dotyczące gwarancji

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego. Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie z wyłączeniem przełączników rdzeniowych i dostępowych. Przełączniki rdzeniowe i dostępowe należy dostarczyć z podstawową gwarancją producenta. Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.