Dokumentacja do projektu

Dostawa urządzeń sieciowych do szkół w ramach projektu "Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin"

Urząd Miasta Lublin

Fundusze Europejskie Program Regionalny
Rzeczpospolita Polska
lubelskie Smakuj życie!
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Spis treści

1. Opis przedmiotu zamówienia

W ramach projektu "Opracowanie i wdrożenie zintegrowanego systemu informatycznego dla jednostek oświatowych miasta Lublin" należy dostarczyć i uruchomić sprzęt aktywny w postaci urządzeń sieciowych rozmieszczonych w poszczególnych jednostkach oświatowych wraz z częścią centralną w postaci koncentratorów zlokalizowanych w serwerowniach Gminy Lublin oraz oprogramowaniem do zarządzania dostarczonymi urządzeniami. Część centralna pozwoli na organizację komunikacji pomiędzy jednostkami, szyfrowanie transmisji oraz zapewnienie komunikacji z siecią Internet. W ramach projektu przewiduje się podłączenie 91 lokalizacji jednostek oświatowych do miejskiej sieci szerokopasmowej. W celu realizacji tego zadania należy dostarczyć urządzenia i zapewnić ich współpracę z miejską siecią szerokopasmową. W ramach umowy należy dostarczyć i skonfigurować urządzenia sieciowe klasy firewall niezbędne do zapewnienia transmisji danych i dostępu do usług w 91 lokalizacjach które zostaną zainstalowane zgodnie z tabelą rozmieszczenia elementów projektu.

Usługa transmisji danych nie jest przedmiotem niniejszego zamówienia i zostanie zapewniona przez Zamawiającego we własnym zakresie.

Zakres przedmiotu zamówienia obejmuje:

- dostawę 91 urządzeń sieciowych do szkół;
- dostawę 2 koncentratorów HUB VPN;
- konfigurację dostarczonych urządzeń;
- instalację i uruchomienie wskazanych urządzeń;
- dostawę systemu zarządzania;
- przeprowadzenie instruktażu stanowiskowego.

1.1. Koncepcja realizacji łączności między placówkami szkolnymi a Urzędem Miasta Lublin

Założenia

- 91 placówek szkolnych
- Placówki szkolne połączone z urzędem miasta Lublin z wykorzystaniem dedykowanej usługi transmisji danych typu L3 lub L2.
- Między placówkami a UML zestawiana jest nakładkowa sieć VPN w topologii gwiazdy z wykorzystaniem protokołu IPsec.
- Hub VPN po stronie UML musi być odporny na awarię pojedynczego urządzenia.
- Hub VPN zapewni Filtrowanie ruchu webowego i deszyfrację tuneli IPsec
- Do zarządzania dostarczonymi urządzeniami uruchomione zostanie centralne logowanie zdarzeń z firewalli w placówkach oraz huba VPN
- Centralne zarządzanie firewallami w placówkach, hubem VPN i centralnymi firewallami UM ze wsparciem dla Role Based Access Control

- Pierwsza linia ochrony DoS oraz polityki QoS realizowane na urządzeniach w placówkach szkolnych.
- Filtrowanie w oparciu o aplikację na urządzeniach w placówkach szkolnych.

Opis koncepcji sieciowej

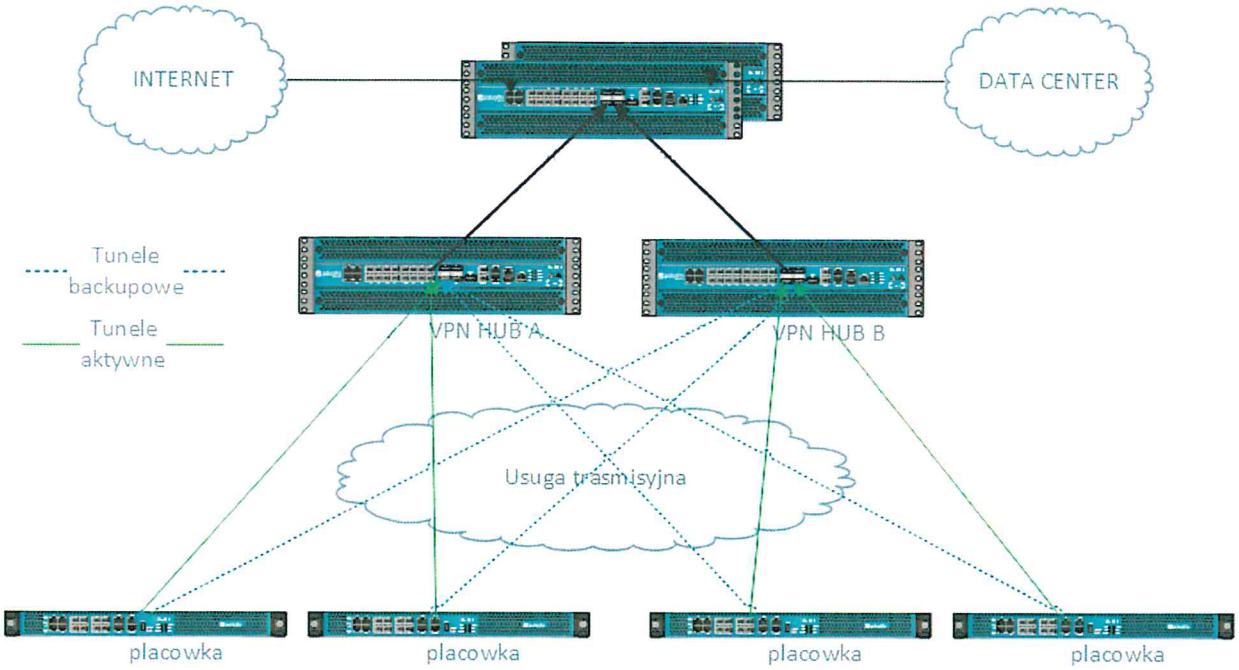
Realizacja ww. założeń wymaga wybudowania redundantnego huba VPN po stronie UM. W skład huba VPN będą wchodzić dwa urządzenia UTM oferujące wydajność firewalla z włączoną funkcją wykrywania aplikacji na poziomie minimum 18Gbps i szyfrowania IPsec 5Gbps. Urządzenia te będą działać jako dwa niezależne koncentratory VPN i będą zarządzane przez centralny system zarządzania. Taka konstrukcja pozwoli w przyszłości rozbudować zagregowaną wydajność huba poprzez rozbudowanie go o kolejne urządzenia. W proponowanym scenariuszu koncentrator A będzie aktywnie obsługiwał ruch z placówek szkolnych 1-45 stanowiąc backup dla placówek 46-91. Podobnie koncentrator B będzie aktywnie obsługiwał ruch z placówek szkolnych 46-91 stanowiąc backup dla palcówek 1-45.

Ruch z placówek można podzielić na dwie klasy: ruch wrażliwy i ruch niewrażliwy. Ruch wrażliwy, to ruch do i z aplikacji dziedzinowych udostępnianych przez UM, który wymaga zapewnienia poufności i integralności. Ruch niewrażliwy, to generyczny ruch do i z Internetu, który nie wymaga dodatkowych form ochrony. Ruch wrażliwy będzie kierowany przez tunel IPsec z włączonym szyfrowaniem (IPsec ESP z szyfrowaniem AES) a ruch niewrażliwy będzie kierowany tunelem z wyłączonym szyfrowaniem (IPsec ESP z szyfrowaniem NULL lub IPsec AH). Kierowanie ruchu pomiędzy tunele będzie realizowane w oparciu o routing dynamiczny i Policy Based Forwarding. Taka segregacja ruchu pomiędzy tunel szyfrowany i nieszyfrowany sprawia, że do wybudowania huba VPN można zastosować tańsze urządzenia o mniejszych wydajnościach IPsec.

Urządzenie w placówce szkolnej w sumie zestawi 4 tunele IPsec: podstawowy i backupowy tunel dla ruchu wrażliwego oraz podstawowy i backupowy tunel dla ruchu niewrażliwego.

Oba koncentratory HUB zostaną podłączone w sposób gwarantujący niezawodność do węzłów Core-1 i Core-2 miejskiej szkieletowej sieci szerokopasmowej. Połączenie nalezy zrealizować przy pomocy portów Ethernet 10Gbps. Oba koncentratory muszą posiadać logiczną łączność z usługami transmisji danych wykorzystywanymi do podłączania placówek szkolnych oraz z centralnymi firewallami.

W placówkach oświatowych należy zainstalować urządzenia UTM o wydajności wydajności firewalla z rozpoznawaniem aplikacji na poziomie 900Mbps i wydajności szyfrowania IPsec 400Mbps.



Rysunek 1 Logiczna topologia nakładkowej sieci VPN

Rozpoznawanie użytkowników

Dostarczone urządzenia należy skonfigurować do współpracy z posiadaną przez Zamawiającego usługą katalogu Active Directory służącego do uwierzytelniania części pracowników w jednostkach oświatowych. Firewalle korzystając z takiego repozytorium mogą rozpoznawać użytkowników i co za tym idzie zezwalają na budowanie dokładnych reguł kontroli dostępu w zależności od roli jaką pełni użytkownika (nauczyciel, uczeń, rodzic).

Inną z metod pozyskania tożsamości użytkownika, którą należy wykorzystać w tym projekcie jest webowy captive portal.

Zarządzanie

Wykonawca dostarczy oprogramowanie do zarządzania grupą 91 urządzeń do jednostek oraz koncentratorów HUB. System zarządzania musi umożliwiać spójne zarządzanie konfiguracją urządzeń, konfiguracją polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur. Dodatkowo musi również pełnić funkcję centralnego repozytorium dla logów generowanych przez wszystkie zarządzane urządzenia. System zarządzania musi zostać dostarczony w formie wirtualnego urządzenia uruchomionego w środowisku VMware ESX, gdzie warstwa wirtualizacyjna zadba o wysoką dostępność systemu zarządzania. Zamawiający zapewni środowisko VMware ESX na potrzeby instalacji systemu zarządzania.

Subskrypcje i licencje

Wykonawca dostarczy wszelkie niezbędne licencje wymagane do realizacji usług: ochrony DoS, obsługi QoS, rozpoznawania aplikacji i użytkowników, zestawiania tuneli IPsec VPN, centralnego systemu zarządzania.

2. Zakres dostawy

Wykonawca dostarczy skonfigurowane urządzenia zgodnie z poniższą tabelą.

2.1. Tabela rozmieszczenia elementów projektu (jednostki oświatowe):

Lp.	Jednostka zewnętrzna	Adres	Urządzenie	Sztuk
1.	Bursa Szkolna nr 1	ul. Księdza Jerzego Popiełuszki 7	Firewall	1
2.	Bursa Szkolna nr 2	ul. Dolna Panny Marii 65	Firewall	1
3.	Bursa Szkolna nr 3	ul. Weteranów 3	Firewall	1
4.	Bursa Szkolna nr 5	ul. Pogodna 52A	Firewall	1
5.	Centrum Kształcenia Ustawicznego nr 2	ul. Pogodna 52	Firewall	1
6.	Szkoła Podstawowa nr 1 im. ks. Stanisława Konarskiego	ul. Kunickiego 116	Firewall	1
7.	XXX Liceum Ogólnokształcące im. księdza Jana Twardowskiego	ul. Wajdeloty 12	Firewall	1
8.	Szkoła Podstawowa nr 33 im. 27. Wołyńskiej Dywizji Piechoty Armii Krajowej	ul. Pogodna 19	Firewall	1
9.	Szkoła Podstawowa nr 15 im. Jana Pawła II	ul. Elektryczna 51	Firewall	1
10.	Szkoła Podstawowa nr 16 im. Fryderyka Chopina	ul. Poturzyńska 2	Firewall	1
11.	Szkoła Podstawowa nr 18 im. Macieja Rataja	Al. Jana Długosza 8	Firewall	1
12.	Szkoła Podstawowa nr 19 im. Józefa Czechowicza	ul. Szkolna 6	Firewall	1

13.	Szkoła Podstawowa nr 5 im. Króla Władysława Łokietka	ul. Smyczkowa 3	Firewall	1
14.	Szkoła Podstawowa nr 57 im. Jana Kochanowskiego	ul, Krasińskiego 7	Firewall	1
15.	XXIX Liceum Ogólnokształcące im. cc mjr Hieronima Dekutowskiego ps. „Zapora"	ul. Lipowa 25	Firewall	1
16.	I Liceum Ogólnokształcące im. Stanisława Staszica	Al. Racławickie 26	Firewall	1
17.	II Liceum Ogólnokształcące im. Hetmana Jana Zamoyskiego	ul. Ogrodowa 16	Firewall	1
18.	III Liceum Ogólnokształcące im. Unii Lubelskiej	Pl. Wolności 4	Firewall	1
19.	IV Liceum Ogólnokształcące im. Stefanii Sem połowskiej	ul. Szkolna 4	Firewall	1
20.	IX Liceum Ogólnokształcące im. Mikołaja Kopernika	ul. Struga 6	Firewall	1
21.	Lubelskie Centrum Kształcenia Zawodowego i Ustawicznego im. Krzysztofa Kamila Baczyńskiego / Zespół Poradni nr 1	ul. Magnoliowa 8	Firewall	1
22.	Młodzieżowy Dom Kultury „Pod Akacją"	ul. Grodzka 11	Firewall	1
23.	Państwowe Szkoły Budownictwa i Geodezji im. Hieronima Łopacińskiego	Al. Racławickie 5	Firewall	1
24.	Specjalny Ośrodek Szkolno-Wychowawczy dla Dzieci i Młodzieży Niepełnosprawnych im. Prof. Zofii Sękowskiej	ul. Hirszfelda 6	Firewall	1
25.	Specjalny Ośrodek Szkolno-Wychowawczy dla Dzieci i Młodzieży Niepełnosprawnych im. Prof. Zofii Sękowskiej	ul. Wyścigowa 31	Firewall	1
26.	Specjalny Ośrodek Szkolno-Wychowawczy dla Dzieci i Młodzieży Niesłyszącej i Słabo Słyszącej im. Jana Pawła II / Poradnia Psychologiczno-Pedagogiczna nr 1	ul. Hanki Ordonówny 4	Firewall	1

27.	Specjalny Ośrodek Szkolno-Wychowawczy nr 1	ul. Aleja Spółdzielczości Pracy 65	Firewall	1
28.	Specjalny Ośrodek Szkolno-Wychowawczy nr 2	ul. Głuska 5	Firewall	1
29.	Szkoła Muzyczna I i II stopnia im. Tadeusza Szeligowskiego	ul. Narutowicza 32a	Firewall	1
30.	Szkoła Podstawowa nr 10 im. Henryka Sienkiewicza	ul. Kalinowszczyzna 70	Firewall	1
31.	Szkoła Podstawowa nr 2 im. Jana Kochanowskiego	ul. Mickiewicza 24	Firewall	1
32.	Szkoła Podstawowa nr 20 im. Jarosława Dąbrowskiego	Al. Piłsudskiego 26	Firewall	1
33.	Szkoła Podstawowa nr 21 im. Królowej Jadwigi	ul. Zuchów 1	Firewall	1
34.	Szkoła Podstawowa nr 23 im. Olimpijczyków Polskich	ul. Podzamcze 9	Firewall	1
35.	Szkoła Podstawowa nr 24 im. Partyzantów Lubelszczyzny / Przedszkole nr 4	ul. Niecała 1	Firewall	1
36.	Szkoła Podstawowa nr 25 im. Władysława Broniewskiego	ul. Sieroca 17	Firewall	1
37.	Szkoła Podstawowa nr 27 im. Marii Montessori - Klasy dotychczasowego Gimnazjum nr 17	ul. Kresowa 1	Firewall	1
38.	Szkoła Podstawowa nr 27 im. Marii Montessori - Klasy dotychczasowego Gimnazjum nr 17	ul. Maszynowa 2	Firewall	1
39.	Szkoła Podstawowa nr 28 z Oddziałami integracyjnymi im. Synów Pułku Ziemi Lubelskiej	ul. Radości 13	Firewall	1
40.	Szkoła Podstawowa nr 28 z Oddziałami integracyjnymi im. Synów Pułku Ziemi Lubelskiej	ul. Romantyczna 11	Firewall	1
41.	Szkoła Podstawowa nr 29 im. Adama Mickiewicza	ul. Wajdeloty 1	Firewall	1
42.	Szkoła Podstawowa nr 3 im. Juliusza Słowackiego	ul. Balladyny 22	Firewall	1

43.	Szkoła Podstawowa nr 30 im. Króla Kazimierza Wielkiego - Klasy dotychczasowego Gimnazjum nr 3 im. prof. Mieczysława A. Krąpca OP	ul. Nałkowskich 110	Firewall	1
44.	Szkoła Podstawowa nr 31 im. Lotników Polskich	ul. Lotnicza 1	Firewall	1
45.	Szkoła Podstawowa nr 32 z Oddziałami Integracyjnymi im. Pamięci Majdanka	ul. Tetmajera 2	Firewall	1
46.	Szkoła Podstawowa nr 34 im. Kornela Makuszyńskiego	ul. Kosmowskiej 3	Firewall	1
47.	Szkoła Podstawowa nr 38 im. Henryka Sienkiewicza	ul. Wołodyjowskiego 13	Firewall	1
48.	Szkoła Podstawowa nr 4 im. Adama Mickiewicza	ul. Hiacyntowa 69	Firewall	1
49.	Szkoła Podstawowa nr 40 im. Leona Kruczkowskiego	ul. Róży Wiatrów 9	Firewall	1
50.	Szkoła Podstawowa nr 42 im. Konstantego Ildefonsa Gałczyńskiego	ul. Rycerska 9	Firewall	1
51.	Szkoła Podstawowa nr 43 im. Ignacego Jana Paderewskiego	ul. Śliwińskiego 5	Firewall	1
52.	Szkoła Podstawowa nr 46 im. Króla Jana III Sobieskiego	ul. Biedronki 13	Firewall	1
53.	Szkoła Podstawowa nr 48 im. Józefa Piłsudskiego	ul. Kasprowicza 112	Firewall	1
54.	Szkoła Podstawowa nr 51 im. Jana Pawła II	ul. Bursztynowa 22	Firewall	1
55.	Szkoła Podstawowa nr 52 im Marii Konopnickiej	ul. Jagiełły 11	Firewall	1
56.	Szkoła Podstawowa nr 6 im. Romualda Traugutta	ul. Czwartaków 11	Firewall	1
57.	Szkoła Podstawowa nr 7 im. ks. Jana Twardowskiego	ul. Plażowa 9	Firewall	1
58.	V Liceum Ogólnokształcące im. Marii Skłodowskiej-Curie	ul. Lipowa 7	Firewall	1
59.	VI Liceum Ogólnokształcące im. Hugona Kołłątaja	ul. Mickiewicza 36	Firewall	1

60.	VIII Liceum Ogólnokształcące im. Zofii Nałkowskiej	ul. Słowicza 5	Firewall	1
61.	XXIII Liceum Ogólnokształcące im. Nauczycieli Tajnego Nauczania	ul. Poniatowskiego 5	Firewall	1
62.	Zespół Szkół Budowlanych im. Eugeniusza Kwiatkowskiego	ul. Słowicza 3	Firewall	1
63.	Zespół Szkół Chemicznych i Przemysłu Spożywczego im. Gen. Franciszka Kleeberga	Al. Racławickie 7a	Firewall	1
64.	Zespół Szkół Ekonomicznych im. A. i J. Vetterów / Młodzieżowy Dom Kultury nr 2	ul. Bernardyńska 14	Firewall	1
65.	Zespół Szkół Elektronicznych	ul. Wojciechowska 38	Firewall	1
66.	Zespół Szkół Energetycznych im. prof. Kazimierza Drewnowskiego	ul. Długa 6	Firewall	1
67.	Zespół Szkół nr 1 im. Władysława Grabskiego	ul. Podwale 11	Firewall	1
68.	Zespół Szkół nr 10	ul. Biedronki 13	Firewall	1
69.	Zespół Szkół nr 11	ul. Farbiarska 8	Firewall	1
70.	Zespół Szkół nr 12	ul. Sławinkowska 50	Firewall	1
71.	Szkoła Podstawowa nr 26 im. Janusza Korczaka	ul. Bronowiska 21	Firewall	1
72.	Zespół Szkół nr 5 im. Jana Pawła II	ul. Elsnera 5	Firewall	1
73.	Zespół Szkół nr 6	ul. Diamentowa 2	Firewall	1
74.	Szkoła Podstawowa nr 50 im. Stefana Kardynała Wyszyńskiego	ul. Roztocze 14	Firewall	1
75.	Szkoła Podstawowa nr 39 im. Szarych Szeregów	ul. Krężnicka 156	Firewall	1
76.	Szkoła Podstawowa nr 47 im. Józefa Ignacego Kraszewskiego	ul. Zdrowa 1	Firewall	1
77.	Zespół Szkół Odzieżowo-Włókienniczych im. Władysława Stanisława Reymonta	ul. Lwowska 11	Firewall	1
78.	Zespół Szkół Ogólnokształcących nr 1 im. Zbigniewa Herberta	ul. Radzyńska 5	Firewall	1

79.	Zespół Szkół Ogólnokształcących nr 2	ul. Przyjaźni 12	Firewall	1
80.	Zespół Szkół Ogólnokształcących nr 4 im. Orląt Lwowskich	ul. Tumidajskiego 6a	Firewall	1
81.	Zespół Szkół Ogólnokształcących nr 5	ul. Rzeckiego 10	Firewall	1
82.	Zespół Szkół Ogólnokształcących nr 6 / Centrum Kształcenia Ustawicznego nr 1 im. Eugeniusza Kwiatkowskiego	ul. Krochmalna 29	Firewall	1
83.	Zespół Szkół Samochodowych im. Stanisława Syroczyńskiego	ul. Długosza 10a	Firewall	1
84.	Zespół Szkół Transportowo-Komunikacyjnych im. Tadeusza Kościuszki	ul. Zemborzycka 82	Firewall	1
85.	Przedszkole nr 12	ul. Wolska 5	Firewall	1
86.	Zespół Poradni nr 2	ul. Żołnierzy Niepodległej 1	Firewall	1
87.	Przedszkole nr 11 Specjalne / Zespół Poradni nr 3	ul. Młodej Polski 30	Firewall	1
88.	Przedszkole nr 77 / Poradnia Psychologiczno-Pedagogiczna nr 2	ul. Radości 8	Firewall	1
89.	Poradnia Psychologiczno-Pedagogiczna nr 3	ul. Rzeckiego 21	Firewall	1
90.	Przedszkole nr 63	ul. Szmaragdowa 22	Firewall	1
91	Przedszkole nr 84	ul. Zygmunta Augusta 17 (wynajem)	Firewall	1

2.2. Tabela rozmieszczenia elementów projektu (część wspólna):

Lp.	Lokalizacja Gminy Lublin	Adres	Urządzenie	Sztuk
1.	Serwerownia numer 1 Urzędu Miasta Lublin (DC 1)	al. Racławicke 5, Lublin	Koncentrator HUB	1
2.	Serwerownia numer 2 Urzędu Miasta Lublin (DC 2)	Plac Łokietka 1, Lublin	Koncentrator HUB	1

3. Wymagania funkcjonalne dostarczanych urządzeń.

3.1. Urządzenie koncentrator HUB VPN

Parametry wymagane

1. System musi być dostarczony jako specjalizowane urządzenie sieciowe (appliance).
2. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
3. System musi umożliwiać działanie w następujących trybach pracy
    a. rutera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (tzn. w warstwie 2 modelu OSI),
    c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
    d. w trybie pasywnego nasłuchu (sniffer).
4. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. System musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF
6. System musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active.
7. Zamawiający wymaga aby produkt był dostępny na rynku co najmniej 6 miesięcy przed terminem składania ofert. Przez „dostępność produktu na rynku" Zamawiający rozumie, iż produkt w postaci konkretnego modelu urządzenia firewall oraz produkt w postaci wskazanej oferowanej wersji firmware (oprogramowanie systemowe) musiał być dostępny w terminie 6 miesięcy przed terminem składania ofert. W przypadku rozwiązania sprzętowego Zamawiający wymaga dostępności w terminie 6 miesięcy przed terminem składania ofert konkretnego modelu urządzenia. Niedopuszczalne jest wskazanie innego urządzenia z typoszeregu czy urządzenia z innej „rodziny".
8. System musi być wyposażony w co najmniej następujące interfejsy sieciowe
    a. 16 portów 1G/10G SFP/SFP+,
    b. 4 porty 40G QSFP+.

10. System musi być wyposażony w co najmniej jeden port konsoli
11. System musi być wyposażony w co najmniej jeden port zarządzający Out-of-Band 10/100/1000

12. System musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
13. System musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,
14. System musi posiadać przepływność w ruchu full-duplex nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering)
15. System musi obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 150000 połączeń na sekundę.
16. System musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 5Gbps.
17. System musi posiadać wbudowane w obudowę co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V.
18. System zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
19. Polityka zabezpieczeń firewall musi uwzględniać
    a. strefy bezpieczeństwa,
    b. adresy IP klientów i serwerów,
    c. protokoły i usługi sieciowe,
    d. aplikacje,
    e. kategorie URL,
    f. użytkowników aplikacji,
    g. reakcje zabezpieczeń,
    h. rejestrowanie zdarzeń i alarmowanie
    i. zarządzanie pasmem w sieci w oparciu o
        i. priorytet,
        ii. pasmo gwarantowane,
        iii. pasmo maksymalne,
        iv. oznaczenia DiffServ
20. System musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
21. System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
22. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji

musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.

23. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
24. System musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
25. System musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
26. System musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
27. System musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
28. System musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
29. System musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci
30. System musi zapewniać integrację z
    a. Active Directory,
    b. Citrix,
    c. LDAP
    d. serwerami Terminal Services
31. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
32. System musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
33. System musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

34. System musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

35. System musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

36. System musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie moze wymagać zakupu dodatkowych licencji.

37. System musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.

38. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

39. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

40. System musi posiadać możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Subskrybcje nie są wymagane.

41. System musi posiadać możliwość rozbudowy o moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje na AV nie są wymagane.

42. System musi posiadać rozbudowy o moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje IPS nie są wymagane.

43. System musi posiadać możliwość rozbudowy o moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje antymalware/antyspyware nie są wymagane.

44. System musi posiadać możliwość rozbudowy o sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. Subskrybcje dla DNS nie są wymagane.

45. System musi zapewniać możliwość rozbudowy funkcjonalonści o przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej

komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Subskrybcje zapewniające taką możliwość nie są wymagane.

46. Zarządzanie systemu musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
47. System musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
48. System musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
49. System musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
50. System musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
51. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
52. System musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
53. System musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej dwie metody uwierzytelniani.
54. System musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się aby do tego celu konieczna była współpraca z zewnętrznymi urządzeniami czy oprogramowaniem.
55. System musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
56. System musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
57. System musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
58. System musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
59. System musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
60. System musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:
    a. ruchu sieciowym,
    b. aplikacjach,
    c. zagrożeniach

d. filtrowaniu stron www.

61. System musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

62. System musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

63. System musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

64. Zamawiajacy wymaga możliwości rozbudowy o następujące subskrybcje/licencje jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego

    a. Subskrybcją na antywirus (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AV)

    b. Subskrybcją na antyspyware (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AS)

    c. Subskrybcją na IPS

    d. Subskrybcją na URL Filtering

    e. Subskrybcja na Remote Access VPN oraz kontrolę stanu stacji

    f. Subskrybcja umożliwiajace przesyłanie plików do chmurowego/lokalnego sandboxa

3.2. Urządzenie firewall do jednostek oswiatowych

1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance).
2. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
3. System zabezpieczeń firewall musi umożliwiać działanie w następujących trybach pracy
    a. rutera (tzn. w warstwie 3 modelu OSI),
    b. przełącznika (tzn. w warstwie 2 modelu OSI),
    c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
    d. w trybie pasywnego nasłuchu (sniffer).
4. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. System zabezpieczeń firewall musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF
6. System zabezpieczeń firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active.
7. Zamawiający wymaga aby produkt był dostępny na rynku co najmniej 6 miesięcy przed terminem składania ofert. Przez „dostępność produktu na rynku" Zamawiający rozumie, iż produkt w postaci konkretnego modelu urządzenia firewall oraz produkt w postaci wskazanej oferowanej wersji firmware (oprogramowanie systemowe) musiał być dostępny w terminie 6 miesięcy przed terminem składania ofert. W przypadku rozwiązania sprzętowego Zamawiający wymaga dostępności w terminie 6 miesięcy przed terminem składania ofert konkretnego modelu urządzenia. Niedopuszczalne jest wskazanie innego urządzenia z typoszeregu czy urządzenia z innej „rodziny".
8. System zabezpieczeń firewall musi być wyposażony w co najmniej następujące interfejsy sieciowe
    a. 4 porty Ethernet 10/100/1000
    b. 8 portów 1G SFP (jeden port SFP obsadzony modułem SFP 1Gb/s LC, 20km)
9. System zabezpieczeń firewall musi być wyposażony w co najmniej jeden port konsoli
10. System zabezpieczeń firewall musi być wyposażony w co najmniej jeden port zarządzający Out-of-Band 10/100/1000

11. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
12. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 900 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji,
13. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 600 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering)
14. System zabezpieczeń firewall musi obsługiwać nie mniej niż 120 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 8000 połączeń na sekundę.
15. System zabezpieczeń firewall musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 400Mbit/s.
16. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
17. Polityka zabezpieczeń firewall musi uwzględniać
    a. strefy bezpieczeństwa,
    b. adresy IP klientów i serwerów,
    c. protokoły i usługi sieciowe,
    d. aplikacje,
    e. kategorie URL,
    f. użytkowników aplikacji,
    g. reakcje zabezpieczeń,
    h. rejestrowanie zdarzeń i alarmowanie
    i. zarządzanie pasmem w sieci w oparciu o
        i. priorytet,
        ii. pasmo gwarantowane,
        iii. pasmo maksymalne,
        iv. oznaczenia DiffServ
18. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
19. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
20. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych.

21. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.

22. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

23. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

24. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

25. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

26. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.

27. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci

28. System zabezpieczeń firewall musi zapewniać integrację z

    a. Active Directory,

    b. Citrix,

    c. LDAP

    d. serwerami Terminal Services

29. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

30. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

31. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

32. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

33. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

34. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.

35. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.

36. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

37. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

38. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Subskrybcje nie są wymagane.

39. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje na AV nie są wymagane.

40. System zabezpieczeń firewall musi posiadać rozbudowy o moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje IPS nie są wymagane.

41. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Subskrybcje antymalware/antyspyware nie są wymagane.

42. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. Subskrybcje dla DNS nie są wymagane.

43. System zabezpieczeń firewall musi zapewniać możliwość rozbudowy funkcjonalonści o przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych

plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Subskrybcje zapewniające taką możliwość nie są wymagane.

44. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.

45. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

46. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.

47. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

48. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

49. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

50. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.

51. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej dwie metody uwierzytelniania.

52. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się aby do tego celu konieczna była współpraca z zewnętrznymi urządzeniami czy oprogramowaniem.

53. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.

54. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.

55. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.

56. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

57. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.

58. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o:

    a. ruchu sieciowym,

    b. aplikacjach,

c. zagrożeniach

d. filtrowaniu stron www.

59. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

60. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

61. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

62. Zamawiajacy wymaga możliwości rozbudowy o następujące subskrybcje/licencje jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego

    a. Subskrybcją na antywirus (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AV)

    b. Subskrybcją na antyspyware (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AS)

    c. Subskrybcją na IPS

    d. Subskrybcją na URL Filtering

    e. Subskrybcja na Remote Access VPN oraz kontrolę stanu stacji

    f. Subskrybcja umożliwiajace przesyłanie plików do chmurowego/lokalnego sandboxa

3.3. System zarządzania

Wymagania ogólne

1. Wraz z systemem zabezpieczeń firewall konieczne jest dostarczenie centralnego systemu zarządzania.
2. System zarządzania, logowania i raportowania musi obsługiwać dostarczone urządzenia oraz docelowo nie mniej niż 200 urządzeń.
3. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej działającej w środowisku VMWare.
4. System zarządzania, logowania i raportowania musi zapewniać współpracy z przestrzenią dyskową o pojemności nie mniejszej niż 4 TB.
5. System zarządzania, logowania i raportowania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie.
6. System zarządzania, logowania i raportowania musi posiadać taki sam Graficzny Interfejs Użytkownika (GUI) jak zarządzane firewalle.
7. System zarządzania, logowania i raportowania musi umożliwiać import obecnej konfiguracji używanych firewalli.
8. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
9. System zarządzania, logowania i raportowania musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
10. System zarządzania, logowania i raportowania musi zapewniać dedykowane narzędzia dla łatwego przeszukiwania skorelowanych logów zebranych z zarządzanych firewalli.
11. System zarządzania, logowania i raportowania musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
12. System zarządzania, logowania i raportowania musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
13. System zarządzania, logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down".
14. System zarządzania, logowania i raportowania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) i globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).

15. System zarządzania, logowania i raportowania musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).
16. System zarządzania, logowania i raportowania musi umożliwiać tworzenie raportów na podstawie zbudowanych kontenerów.
17. System zarządzania, logowania i raportowania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
18. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
19. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek.
20. System zarządzania, logowania i raportowania musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
21. System zarządzania, logowania i raportowania musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne).
22. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
23. System zarządzania, logowania i raportowania musi informować o zmianach konfiguracji systemu.
24. System zarządzania, logowania i raportowania musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem.
25. System zarządzania, logowania i raportowania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.
26. System zarządzania, logowania i raportowania musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał iż nowe urządzenie zastępuje urządzenie uszkodzone.
27. System zarządzania, logowania i raportowania musi być dostarczony jako dedykowane urządzenie/urządzenia sieciowe.
28. System zarządzania, logowania i raportowania musi móc pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów.
29. System zarządzania, logowania i raportowania musi zapewniać możliwość rozbudowy systemu o kolejne urządzenia tak aby umożliwić zwiększenie pojemności lub/i wydajności całego systemu w przyszłości.

4. Testy

4.1. Testy weryfikujące

W ramach postępowania Zamawiający wymaga przeprowadzenia testów weryfikujących oferowanych rozwiązań obowiązkowo przed wyborem oferty. Celem przeprowadzenia procedury testowej jest weryfikacja zgodności urządzeń i oprogramowania z wymaganiami. Wszelkie testy będą przeprowadzane przez Wykonawcę na jego koszt i ryzyko. Wykonawca będzie zobowiązany do dostarczenia na potrzeby testów egzemplarza wzorcowego oferowanego rozwiązania obejmującego:

1. Oferowane urządzenia:
   1.1. Koncentrator HUB VPN
   1.2. Firewall do jednostek oświatowych
2. Platformę sprzętową umożliwiającą uruchomienie niezbędnych komponentów,
3. Wymagane do uruchomienia powyższych elementów licencje (dopuszczalne wersje testowe bez ograniczeń funkcjonalnych ważne w okresie trwania testów),
4. Kompletną dokumentację dostarczanych elementów i systemów w języku polskim lub angielskim (lub wskazanie publicznie dostępnych stron internetowych z lokalizacją dokumentacji).

Testy zostaną przeprowadzone w środowisku laboratoryjnym, aby zmaksymalizować dostępność urządzeń i możliwość ich rekonfiguracji do potrzeb danego scenariusza testowego. Zamawiający zapewni środowisko laboratoryjne, spełniające typowe wymagania pracy urządzeń aktywnych (kontrola parametrów środowiskowych, szafy rack 19" do instalacji urządzeń, zasilanie gwarantowane). Zamawiający zastrzega możliwość weryfikacji wszystkich parametrów i funkcjonalności w odniesieniu do każdego z wymogów.

Opis procedury testowej

Testy odbędą w serwerowni przy Al. Racławickie 5 w Lublinie. Wykonawca będzie zobowiązany do dostarczenia tam urządzeń podlegających testom w ustalonym terminie oraz odebrania ich po zakończeniu procedury testowej. Wszystkie testy odbywać się będą w obecności przedstawicieli Zamawiającego, oraz przedstawicieli Wykonawcy. Wszystkie przeprowadzone testy muszą dać mierzalne wyniki – w przypadku zaobserwowania niestabilności pracy urządzeń lub funkcjonalności, wymagane jest powtórzenie testu. Jeżeli praca urządzeń zostanie ustabilizowana (trzykrotne powtórzenie testu da powtarzalne wyniki), w takim przypadku test zostanie zaliczony.

4.2. Urządzenia testujące

Testy muszą zostać wykonane dedykowanym urządzeniem typu „appliance" umożliwiającym wygenerowanie ruchu większego niż wymagany w procedurze testowej, a także umożliwiające generowanie ruchu na podstawie pliku zawierającego podsłuchany (za pomocą sniffera) rzeczywisty ruch występujący w sieci Zamawiającego. Urządzenie testujące musi być dostarczone przez Wykonawcę. Wymagania co do urządzenia testującego:

1) Urządzenie generujące ruch musi mieć możliwość testowania parametrów wydajnościowych urządzeń sieciowych takich jak przełączniki, routery, firewalle.
2) Urządzenie generujące ruch musi symulować pracę zarówno klienta jak i serwera dla testowanych aplikacji (odbiornik, nadajnik).
3) Urządzenie musi pozwalać (w przypadku przeprowadzenia testu firewalla) na wykonanie testów w trybie bridge (L2) jak i w trybie routing (L3).
4) Urządzenie musi mieć możliwość wygenerowania ruchu o wolumenie większym, niż wymagany przez Zamawiającego maksymalny wolumen ruchu dla oferowanego urządzenia.
5) Urządzenie musi posiadać predefiniowane przez producenta próbki symulujące ruch generowany prze różnego rodzaju aplikacje, grupy aplikacji oraz protokoły HTTP Enterprise, Windows Update, Facebook, Google Email, Microsoft Exchange, Oracle, Enterprise Mix.
6) Urządzenie musi mieć możliwość wygenerowania ruchu dla wybranej grupy aplikacji, o określonym wolumenie i określonej liczbie symulowanych użytkowników.
7) Urządzenia powinno posiadać możliwość automatycznego przerwania testu, jeśli liczba błędów przekroczy określoną wartość.
8) W czasie prowadzonego testu urządzenie musi na bieżąco raportować informacje o generowanym ruchu. W czasie testu powinny być dostępne takie informacje jak:
    a. sumaryczny wolumen generowanego ruchu,
    b. wolumen ruchu na poszczególnych interfejsach,
    c. liczba wygenerowanych transakcji (poprawne oraz nieudane),
    d. liczba wygenerowanych sesji TCP, liczba jednoczesnych sesji TCP, liczba sesji TCP/sec.
9) Po zakończeniu testów urządzenie musi wygenerować raport z wykonanego testu zawierający conajmniej informacje o:
    a. wolumenie wygenerowanego ruchu,
    b. procentowym udziale poszczególnych aplikacji w wolumenie generowanego ruchu,
    c. ilości błędów w generowanym ruchu,
    d. liczbie wygenerowanych sesji TCP,
    e. ruchu wygenerowanym na poszczególnych interfejsach.

Generator powinien symulować rzeczywisty ruch występujący w sieci klienta/w sieciach typu enterprise.

4.3. Procedura testów urządzeń typu koncentrator HUB VPN oraz firewall

Testy muszą zostać wykonane dedykowanym urządzeniem typu „appliance" umożliwiającym wygenerowanie ruchu o wymaganej charakterystyce i wolumenie, a także umożliwiające generowanie ruchu na podstawie pliku zawierającego podsłuchany (za pomocą sniffera) rzeczywisty ruch występujący w sieci Zamawiającego. Zamawiający dopuszcza możliwość wykorzystania gotowych próbek zaimplementowanych w dedykowanym urządzeniu typu appliance.

Wymagania na urządzenie testujące zostało opisane powyżej

Wymagania wobec testów oraz procedura ich przeprowadzenia:

1. Wykonawca w terminie wykonania testów musi przekazać Zamawiającemu kompletne środowisko testowe, w szczególności sprzęt i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów. Po wykonaniu prezentacji Wykonawca zabierze dostarczone przez siebie urządzenia.
2. Miejsce i sposób przeprowadzenia testów:

a. Testy odbywać się będą w serwerowni przy Al. Racławickie 5 w Lublinie. O terminie przeprowadzenia testów Wykonawca zostanie poinformowany osobnym pismem.

b. Czas trwania testów nie może być dłuższy niż 6 godzin zegarowych. Wykonawca będzie miał prawo przygotowania środowiska testowego w miejscu testów dwie godziny zegarowe przed początkiem testów. Czas ten może zostać wykorzystany przez Wykonawcę do przygotowania się do testów.

c. W celu realizacji testów (podczas przygotowania oraz przeprowadzenia) Wykonawca może korzystać wyłącznie ze środowiska testowego przez siebie dostarczonego. Wyjątek stanowią tutaj urządzenia prezentacyjne: rzutnik, ekran, monitor.

d. Podczas testów Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane funkcjonalności.

e. W przypadku wystąpienia podczas testów problemów lub błędów Wykonawca ma prawo do podjęcia czynności zmierzających do ich eliminacji/usunięcia, w szczególności może dokonywać niezbędnych z jego punktu widzenia modyfikacji prezentowanego środowiska testowego, w ramach czasu przewidzianego na testy, o którym mowa w ppkt. b powyżej. Po przekroczeniu czasu na testy, tj. po upływie 6 godzin zegarowych, zadania które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane.

f. Testy muszą być prowadzone w języku polskim.

5. Generator powinien wygenerować ruch na podstawie pliku zawierającego ruch pozyskany przez Zamawiającego w jego sieci poprzez sniffing. Plik z ruchem zostanie dostarczony przez Zamawiającego Wykonawcy przed rozpoczęciem testów. Zamawiający dopuszcza możliwość wykorzystania gotowych próbek zaimplementowanych w dedykowanym urządzeniu typu appliance w celu wygenerowania ruchu - do testów należy przyjąć profil ruchu typu „Enterprise MIX".

6. Stan wyjściowy:

a. Test powinien zostać wykonany bez urządzeń na ścieżce ruchu – porty nadajnika i odbiornika połączone bezpośrednio. W ramach testu należy wygenerować ruch zgodnie ze specyfikacją

Przebieg testu:

Lp.	Nazwa testu	Opis	Oczekiwany wynik	Wynik pozytywny (tak / nie)
1.	Weryfikacja konfiguracji generator – 15 Gbps	Generowanie ruchu o wolumenie 15 Gbps na podstawie pliku z ruchem Zamawiającego lub gotowych próbek zaimplementowanych w dedykowanym urządzeniu *) czas trwania testu – 5 min	Potwierdzenie uzyskanych wyników w statystykach generatora oraz w raporcie końcowym.	

*) Sumaryczny ruch (Tx + Rx)

Testy urządzeń z użyciem generatora, Przebieg testu:

Dla każdego z oferowanych typów urządzeń zostaną zmierzone parametry wydajnościowe. W przypadku testu wydajności szyfrowania testowana będzie para urządzeń.

Lp.	Nazwa testu	Opis	Oczekiwany wynik	Wynik pozytywny (tak / nie)
1.	Test wydajności	Generacja ruchu o wolumenie zgodnyn z wymaganiami dla testowanego urządzenia *) czas trwania testu – 5 min Włączona pełna funkcjonalność urządzenia (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL)	Poprawne działanie urządzenia, prawidłowa kategoryzacja ruchu	

2	Test wydajności szyfrowania	Generacja ruchu o wolumenie zgodnyn z wymaganiami dla testowanego urządzenia*) czas trwania testu – 5 min Włączona pełna funkcjonalność urządzenia (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL)	Poprawne działanie urządzenia, prawidłowa kategoryzacja ruchu	

*) Sumaryczny ruch (Tx + Rx)

5. Zakres wdrożenia

Dostawa urządzeń zgodnie z tabelą rozmieszczenia elementów projektu

Wykonawca dostarczy sprzęt we wskazanych w projekcie lokalizacjach na własny koszt. Wszystkie urządzenia zostaną przekazane na stan zamawiającego w momencie podpisania protokołu odbioru.

Instalacja, konfiguracja i uruchomienie koncentratorów VPN w sieci zamawiającego

Instalacja urządzeń odbędzie się pod nadzorem osób wskazanych przez Zamawiającego w terminach uzgodnionych z Zamawiającym. Wykonawca dostarczy wszelkie niezbędne akcesoria oraz okablowanie niezbędne do uruchomienia dostarczonego sprzętu w tym moduły QSFP niezbędne do podłączenia dostarczonych udządzeń do sieci Zamawiającego. Zamawiający udostepni porty QSFP na posiadanych urządzeniach do których należy podłączyć dostarczaną infrastrukturę. Komunikacja w obrębie rdzenia bedzie oparta o dedykowane połączenia światłowodowe i technologię 40Gbps z zapewnieniem redundancji. Wykonawca skonfiguruje urządzenia zgodnie z wyżej opisaną koncepcją. Wykonawca oznaczy urządzenia naklejką z logotypami zgodnie z zasadami oznakowania projektów współfinansowanych w ramach RPO WL na lata 2014- 2020. Wzór naklejki zostanie uzgodniony z Zamawiającym.

Konfiguracja i uruchomienie urządzeń firewall, wdrożenie stanowiskowe

Instalacja urządzeń odbędzie się pod nadzorem osób wskazanych przez Zamawiającego w terminach uzgodnionych z Zamawiającym. Wykonawca dostarczy wszelkie niezbędne akcesoria oraz okablowanie niezbędne do uruchomienia dostarczonego sprzętu w tym moduły SFP niezbędne do podłączenia dostarczonych urządzeń do sieci Zamawiającego. Wykonawca skonfiguruje urządzenia zgodnie z wyżej opisaną koncepcją. Wykonawca uruchomi urządzenia w 20 wskazanych przez Zamawiającego lokalizacjach. Wykonawca oznaczy urządzenia naklejką z logotypami zgodnie z zasadami oznakowania projektów współfinansowanych w ramach RPO WL na lata 2014- 2020. Wzór naklejki zostanie uzgodniony z Zamawiającym.

Wykonawca po zakończeniu instalcji i konfiguracji urządzeń przygotuje dokumentację powykonawczą.

6. Procedura odbiorowa

Po zakończeniu prac wdrożeniowych zostanie przeprowadzona procedura odbioru działającej instalacji. Celem procedury weryfikacyjnej jest sprawdzenie poprawności działania i konfiguracji komponentów wchodzących w skład infrastruktury objętej niniejszym postępowaniem przetargowym. W szczególności zostaną wykonane następujące prace:

Infrastruktura fizyczna

1. Montaż urządzeń infrastruktury:
    1.1. Sprawdzenie poprawności instalacji urządzeń infrastruktury pod kątem montażu fizycznego, zgodnie z zaleceniami producenta (chłodzenie, zasilanie, odległość montażowa w szafach).
    1.2. Sprawdzenie poprawności oznakowania urządzeń w szafach montażowych.
    1.3. Sprawdzenie poprawności wykonania okablowania i oznakowania w obrębie szaf montażowych.
    1.4. Ocena estetyki montażu.
2. Komponenty zasilania infrastruktury:
    2.1. Sprawdzenie poprawności podłączeń faz zasilania.
    2.2. Sprawdzenie poprawności podłączeń zasilaczy redundantnych.
    2.3. Sprawdzenie bezprzerwowej pracy urządzeń w przypadku awarii pojedynczej linii zasilającej.
3. Zarządzanie urządzeniami ze stacji zarządzającej:
    3.1. Sprawdzenie systemu zarządzającego do urządzeń wymaganych przez SIWZ.
4. Dostęp do sieci Internet z urządzeń sieciowych:
    4.1. Sprawdzenie działania dostępu do sieci Internet.
    4.2. Weryfikacja tablicy routingu.
5. Weryfikacja komunikacji w obrębie wdrożonej infrastruktury:
    5.1. Sprawdzenie łączności IP pomiędzy urządzeniami.
    5.2. Sprawdzenie poprawności routingu IP w sieci.
    5.3. Sprawdzenie poprawności działania redundancji w sieci.
    5.4. Weryfikacja tablicy routingu sieci w poszczególnych obszarach sieci.
    5.5. Wyłączenie urządzeń redundantnych i weryfikacja dostępności komunikacji.
    5.6. Sprawdzenie poprawności działania infrastruktury i wydajności.
6. Weryfikacja zgodności dokumentacji powykonawczej z wdrożoną infrastrukturą.
    6.1. Weryfikacja zestawienia urządzeń.
    6.2. Weryfikacja schematów połączeń
    6.3. Weryfikacja planu adresacji.
    6.4. Weryfikacja konfiguracji urządzeń.

Rezultaty ww. czynności zostaną opisane w dokumencie zawierającym podsumowanie prac związanych z odbiorem infrastruktury. Dokument ten musi zostać zatwierdzony przez Zamawiającego.

Do protokołu odbiorowego Wykonawca załączy:

1. Zaakceptowaną przez Zamawiającego dokumentację powykonawczą
2. Oryginały dokumentów poświadczające gwarancję producenta świadczoną na rzecz Zamawiającego na okres gwarancji na przedmiot umowy.
3. Dokumenty potwierdzające przeprowadzenie instruktaży stanowiskowych Dokumenty potwierdzające wykupienie wszelkich obowiązkowych subskrypcji oraz licencji niezbędnych do funkcjonowania dostarczonej infrastruktury teleinformatycznej na okres gwarancji
4. Zamawiający wymaga załączenia do końcowego protokołu odbioru dla każdego dostarczanego urządzenia/materiału Certyfikatu Pochodzenia lub innego dokumentu wystawionego przez producenta lub jego lokalnego przedstawiciela (zawierającego między innymi dane identyfikacyjne produktu pozwalające na jego identyfikację: kod produktu, nr seryjny) potwierdzający, że dany dostarczony produkt jest fabrycznie nowy, jest oznakowany symbolem CE, pochodzi z autoryzowanej sieci sprzedaży – oficjalnego kanału sprzedaży na rynek europejski.

7. Instruktaż stanowiskowy

Wykonawca zapewni Zamawiającemu instruktaż stanowiskowy oferowanych produktów w wymiarze 16 godzin dla 4 osób. Instruktaż będzie przeprowadzony w w języku polskim.