Załącznik nr 1 do Zapytania ofertowego - SOPZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa ochrony sieci OSE przed atakami typu DDoS (Distributed Denial of Service), zwana dalej Usługą, wraz z usługą instruktażu.

Usługa świadczona na rzecz NASK musi chronić infrastrukturę sieci OSE przed wszystkimi rodzajami ataków typu DDoS wolumetrycznych i aplikacyjnych, a w szczególności:

- powodującymi przepełnienie i wysycenie pasma potrzebnego do świadczenia usług;
- mającymi na celu zalanie pakietami IP;
- powodującymi wyczerpanie zasobów systemu świadczącego usługę np. przez zalanie pakietami z flagą TCP SYN;
- atakami z wykorzystaniem dużej ilości sesji na konkretną aplikację wykorzystywaną do świadczenia usługi;

W przypadku wystąpienia ataku typu DDoS działanie Usługi będzie polegało, na przesłaniu na punkt styku pomiędzy Wykonawcą a Zamawiającym, o którym mowa w ust. 2.2. ruchu oczyszczonego. W przypadku wystąpienia ataku, bez znaczenia jakiej skali i jakiego typu, objętego ochroną Usługi, Zamawiający będzie otrzymywał ruch produkcyjny, z wymaganą jakością czyszczenia w stosunku do określonego wolumenu ruchu.

Usługa ma działać w dwóch, uzupełniających się trybach:

- w trybie „na żądanie”, tj. Zamawiający po wykryciu ataku typu DDoS przekieruje ruch na Wykonawcę w celu oczyszczenia ruchu.
- w trybie ciągłym, kiedy to ataki typu DDoS są automatycznie wykrywane przez infrastrukturę Wykonawcy i oczyszczanie ruchu jest uruchamiane bez dodatkowego udziału Zamawiającego.

Szczegóły realizacji Usługi w obydwóch trybach zostały opisane w ust 2 poniżej.

Usługa będzie zamawiana z określoną przepustowością, definiującą ilość czyszczonego ruchu przychodzącego na stykach z infrastrukturą Wykonawcy. W trakcie trwania Umowy Zamawiający będzie mógł zwiększać przepustowość Usługi.

Usługa będzie świadczona przez 12 miesięcy od dnia podpisania protokołu odbioru usługi.
Zamawiający przewiduje możliwość skorzystania z prawa opcji, które będzie polegało na wydłużeniu przez Zamawiającego czasu realizacji usługi ochrony sieci OSE przed atakami typu DDoS, o dalszych 6 miesięcy, 2 razy po 6 miesięcy lub 12 miesięcy, ponad okres objęty zamówieniem podstawowym.
Zamawiający ma możliwość skorzystania z prawa opcji w terminie nie krótszym niż 2 tygodnie przed datą upływu okresu obowiązywania Umowy wskazanego w ust. 5 lub przed datą upływu okresu realizacji Usługi wskazanego w pierwszym pisemnym oświadczeniu o skorzystaniu z prawa opcji, w przypadku skorzystania z prawa opcji o dalszych 6 miesięcy lub w wariancie 2 razy po 6 miesięcy.

2. Sposób technicznej realizacji Usługi

2.1. Miejsce świadczenia Usługi

Usługa będzie świadczona na portach urządzenia brzegowego Zamawiającego, w budynku DC Praga, ul. 11 Listopada 23 w Warszawie.
Zamawiający dedykuje na potrzeby realizacji Usługi port 100GE w urządzeniu (routerze) OSE pracując w standardzie 100GBase-LR4.

2.2. Dołączenie do sieci Zamawiającego

Zamawiający wymaga realizacji Usługi zgodnie z poniższym opisem:
Punkt styku pomiędzy Wykonawcą a Zamawiającym, wykorzystywany do świadczenia Usługi, będzie zrealizowany we wskazanym w ust. 2.1 powyżej miejscu instalacji urządzenia Zamawiającego. Wykonawca zestawi łącze światłowodowe, doprowadzone do MMR ww. lokalizacji.
Koszt zestawienia łącza i utrzymania łącza przez okres trwania Umowy ponosi Wykonawca w ramach wynagrodzenia z tytułu w świadczenia Usługi.

2.3. Infrastruktura adresowa Zamawiającego

Zamawiający posiada własny, publiczny numer AS oraz realizuje routing do i z Internetu przy wykorzystaniu protokołu BGP. Zamawiający wykorzystuje w własne pule adresów publicznych IPv4 (od jednej do ośmiu pul adresowych o rozmiarach od /17 do /21, przy czym każda pula może mieć inny rozmiar) oraz IPv6 (rozmiar puli /32). Zamawiający przekaże informacje techniczne dotyczące używanej w sieci oraz podlegającej ochronie adresacji IP w trybie roboczym.
Wykonawca zmodyfikuję konfigurację usługi w zakresie dostosowania usługi do zmiany używanych przez Zamawiającego pul adresowanych IPv4, w ciągu 3 (trzech) dni roboczych od przekazania przez Zamawiającego informacji o zmianie tych pul adresowych.

2.4. Skalowanie rozwiązania

W chwili uruchomienia Usługi zestawione zostanie łącze 100GE. Zamawiający będzie monitorował wykorzystanie własnych styków z Internetem.
Zamawiający uruchomi Usługę z przepustowością 30Gb/s ruchu oczyszczonego. Zamówienia na zwiększanie ruchu będą przesyłane do Wykonawcy nie częściej niż 1 raz na 2 tygodnie. Zwiększenie przepustowości nastąpi w ciągu 3 (trzech) dni roboczych od dnia złożenia zamówienia.
Zwiększenie przepustowości może nastąpić w dowolnym momencie okresu rozliczeniowego. Zamawiający będzie zwiększał przepustowość Usługi o 10Gb/s lub jego wielokrotność, do maksymalnej przepustowości 100Gb/s.
Zamawiający szacuje następujący wzrost przepustowości w trakcie trwania Umowy

Miesiąc świadczenia Usługi	0*	1	2	3	4	5	6	7	8	9	10	11	12
Szacowana łączna przepustowość Usługi [Gb/s]	30	30	30	40	40	40	40	40	40	40	50	50	50

Miesiąc świadczenia Usługi	-	13	14	15	16	17	18	19	20	21	22	23	24
Szacowana łączna przepustowość Usługi [Gb/s]	-	50	50	50	60	60	60	70	70	70	80	90	100

*) w momencie uruchomienia usługi

Miesiące 0 - 12 dotyczą wzrostu przepustowości w zakresie trwania zamówienia podstawowego, a miesiące 13 - 24 w zakresie trwania maksymalnego zamówienia w ramach prawa opcji.

3. Parametry usługi

Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny i Wykonawca zobowiązany jest do ich spełnienia w ramach ceny oferowanej Usługi. Wszystkie wymienione parametry muszą być spełniane łącznie.

3.1. Opis usługi

Usługa będzie świadczona dla całej adresacji IP wskazanej przez Zamawiającego.
Infrastruktura Wykonawcy musi zapewnić geolokalizację adresów IP umożliwiającą blokadę ruchu przychodzącego z danego kraju bądź obszaru geograficznego.
W ramach realizacji Usługi Zamawiający wymaga zapewnienia co najmniej:

a. analizy ruchu w celu identyfikacji typu i natury ataku, wykonywanej na podstawie danych zebranych z trzech urządzeń Zamawiającego, w oparciu o technologię netflow, IPFIX lub inną ustalaną przez Strony w trybie roboczym,
b. powiadamiania Zamawiającego o podejrzeniu wystąpienia ataku,
c. rozpoczęcia usuwania ataku w porozumieniu z Zamawiającym (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia),
d. modyfikacji zestawu użytych mechanizmów przeciwdziałania w celu nieuzyskania maksymalnego poziomu filtracji ruchu niepożądanego, przy minimalnym wpływie na ruch prawidłowy,
e. klasyfikacji ataków typu DDoS jako:
    - zweryfikowany atak,
    - fałszywy alarm,
    - nagły ruch – znaczący wzrost ruchu spowodowany inną przyczyną niż atak na daną usługę Zamawiającego.

3.2. Wykrywanie zagrożeń

Wykonawca zapewni efektywną identyfikację potencjalnych ataków typu DDoS z wykorzystaniem poniższych mechanizmów:

a. detekcja sygnatury,
b. przekroczenie progów ruchu dla określonych typów pakietów i protokołów,
c. wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu oparte na analizie profilu ruchu Zamawiającego.

Wykonawca zapewni wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, błędnych pakietów IP /TCP, fragmentowanych pakietów IP, DNS, pakietów adresowanych prywatnymi adresami IP, UDP.
Infrastruktura Wykonawcy, realizująca Usługę, na podstawie danych historycznych musi wyznaczać oczekiwaną wartość ruchu do chronionej podsieci o danej porze dnia w danym dniu tygodnia, w odniesieniu do poszczególnych usług Zamawiającego.
Wykonawca zapewni wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu oraz wykrywanie potencjalnych ataków w warstwie aplikacyjnej dla poszczególnych usług Zamawiającego w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu.

3.3. Oczyszczanie ruchu

Usługa musi zapewniać ochronę infrastruktury Zamawiającego przed atakami typu DDoS poprzez usuwanie niewłaściwego ruchu ze strumienia ruchu kierowanego do Zamawiającego z Internetu. Oczyszczanie ruchu powinno mieć minimalny wpływ na ruch uprawniony (brak tzw. false positives, tj. wskazywania uprawnionego ruchu jako przeznaczonego do odrzucenia).
Efektywne działanie powinno obejmować:

a. przekierowanie do dedykowanych do tego celu zasobów Wykonawcy, w razie podejrzenia wystąpienia ataku na ruch przychodzący do Zamawiającego
b. filtrowanie ruchu oparte o wielowarstwową analizę i mechanizmy przeciwdziałania,
c. kierowanie oczyszczonego ruchu do sieci Zamawiającego.

Zamawiający wymaga oczyszczania ruchu z wszystkich typów ataków występujących w sieci, wykrywanych w danym momencie przez infrastrukturę Wykonawcy, w tym następujących typów ataków:

- TCP SYN flood,
- UDP flood (w tym DNS reflection),
- HTTP GET flood,
- HTTP POST flood,
- ICMP flood,
- IGMP flood,
- invalid packets,
- IP fragments,
- IP NULL,
- DNS flood,
- SIP request flood,
- SSL negotiation,
- NTP flood (w tym NTP reflection,).

3.4. Przerwanie czyszczenia ruchu (ang. Fall-Back Procedure)

Jeśli uruchomione czyszczenie ruchu (eliminacja ataku typu DDoS) ma negatywny wpływ na chronione zasoby lub usługi, Zamawiający będzie mieć możliwość zlecenia jego przerwania, co nastąpi w ciągu 10 minut od momentu złożenia zlecenia przez Zamawiającego.
Pomimo przerwania czyszczenia ruchu, ruch Zamawiającego cały czas podlega monitorowaniu i istnieje możliwość przywrócenia mechanizmów obronnych w odpowiednio dostosowanym zakresie i analogicznym czasie wdrożenia.

4. SLA dla Usługi i komunikacja

4.1. Komunikacja

W ramach świadczonej Usługi istnieje konieczność komunikowania się pomiędzy Wykonawcą, a Zamawiającym. Przypadki, w jakich występuje konieczność komunikacji zostały opisane w ust. 4.2 poniżej. Zamawiający i Wykonawca będą używali następujących kanałów komunikacji:

a. Telefon,
b. Poczta elektroniczna,
c. SMS na telefon komórkowy.

Wykonawca i Zamawiający będą stosowali następujący scenariusz komunikacji:

a. Potwierdzanie automatycznego blokowania ataku – poczta elektroniczna,
b. Zgłaszanie zlecenia filtrowania ruchu – telefon,
c. Zgłaszanie przerwania czyszczenia ruchu- telefon,
d. Eskalacja w przypadku braku kontaktu poprzez pocztę elektroniczną lub telefon – sms na grupę telefonów komórkowych.

4.2. Powiadamianie o ataku

1) Czas Reakcji na Atak (CRA):
   a. Przez CRA rozumie się czas, jaki upłynie od wykrycia ataku typu DDoS do skutecznego poinformowania Zamawiającego z użyciem ustalonych kanałów komunikacji.
   b. Przez skuteczne powiadomienie Zamawiającego rozumie się w szczególności rozmowę z Zamawiającym oraz jego autoryzację.
   c. CRA liczony jest od momentu zaraportowania ataku na platformie zarządzającej infrastrukturą świadczącą Usługę, do czasu zarejestrowania w systemie teleinformatycznym Wykonawcy czasu dokonania pierwszej czynności mającej na celu poinformowanie Zamawiającego przy użyciu wybranego kanału komunikacyjnego.
   d. Każda próba kontaktu będzie wykonywana przez Wykonawcę co dwie minuty w maksymalnym czasie łącznym CRA. Jeśli nie dojdzie do skutecznego kontaktu w pierwszej próbie, Wykonawca zobowiązany jest do wykonania następnej próby wg. zdefiniowanego scenariusza działań. W przypadku niemożności uzyskania połączenia z Zamawiającym w CRA we wszystkich próbach kontaktu, Wykonawca wykorzystuje ostatnią formę komunikacji zgodnie ze scenariuszem działań.
   e. W przypadku ochrony na żądanie, ochrona nie będzie włączona do momentu skutecznego kontaktu z Zamawiającym i potwierdzenia decyzji o włączeniu lub nie włączeniu ochrony.
   f. Wartość CRA wynosi 15 minut.
2) Czas Reakcji na Zlecenie oczyszczania ruchu (CRZ):
   a. Przez CRZ rozumie się czas, jaki upłynie od przyjęcia Zlecenia od Zamawiającego z żądaniem włączenia lub wyłączenia oczyszczania po zarejestrowanym ataku, do momentu rozpoczęcia lub zakończenia oczyszczania ruchu.
   b. Wartość CRZ wynosi 15 minut.
3) Czas rozpoczęcia automatycznego czyszczenia (CRAC)
   a. Czas od momentu zaistnienia ataku do momentu skutecznej jego mitygacji.
   b. Wartość CRAC wynosi 5 minut

4.3. Alarmy i sposób powiadamiania Zamawiającego:

Wykryte w ramach realizacji Usługi zdarzenia zostaną przyporządkowane do jednej z niżej opisanych grup alarmów:

Kategoria alarmu	Opis zdarzenia	Akcja / Czas reakcji
KRYTYCZNA **(Servity High)**	Alarm o wolumenie ataku powyżej 10Gb/s oraz każdy atak aplikacyjny.	Automatycznie rozpoczęcie akcji oczyszczania. Do Zamawiającego zostanie wysłane powiadomienie o zaistnieniu ataku typu DDoS w czasie zdefiniowanym w Umowie.
WAŻNA **(Servity Medium)**	Inne ataki typu DDoS, nie zawarte w kategorii „Krytyczna”.	Poinformowanie Zamawiającego o stwierdzonym ataku i podjęcie działań, zgodnie z wymaganiami Zamawiającego.
INFORMACYJNA **(Servity Low)**	Zapis informacji o ataku.	Brak działania. Brak konieczności informowania Zamawiającego.

4.4. Przywrócenie stanu sprzed ataku

Wykonawca przywróci ruch do stanu normalnego w czasie nie dłuższym niż 30 minut od zakończenia ataku i poinformuje o tym fakcie Zamawiającego.

4.5. Skuteczność czyszczenia ruchu

Skuteczność Usługi w zakresie filtrowania ruchu będzie nie niższa niż 90% w skali okresu rozliczeniowego, w efekcie Zamawiający dopuszcza przejście maksymalnie do 10% ruchu niewłaściwego (ataku) z całego wolumenu ruchu, przez systemy Wykonawcy i skierowanie tego ruchu do sieci Zamawiającego.

4.6. Dostępność Usługi

Wykonawca zapewni dostępność Usługi, rozumianej jako gotowość infrastruktury Wykonawcy do świadczenia Usługi na poziomie 99,9% w skali okresu rozliczeniowego.

4.7. Terminy realizacji Usługi

W zakresie wdrożenia Usługi oraz zmiany przepustowości Wykonawca będzie zobowiązany do dotrzymania poniższych terminów:

1.	Czas na przygotowanie Projektu wykonawczego	5 dni roboczych od daty podpisania umowy
2.	Czas na wdrożenie Usługi	14 dni od daty akceptacji Projektu wykonawczego
3.	Czas na zwiększenie przepustowości	3 dni robocze od daty złożenia zamówienia
4.	Czas na przekazanie dokumentacji powykonawczej	7 dni od daty podpisania Protokołu Odbioru Wdrożenia Usługi

5. Portal administracyjny i raporty

5.1. Funkcjonalności portalu

Wykonawca musi udostępnić Zamawiającemu dostęp do portalu oferujący następujące funkcjonalności:

a. Panel zarządzający Usługą, pozwalający w szczególności na:
   - dostęp do raportów generowanych przez system,
   - dostęp do listy wykrytych ataków,
   - dostęp do listy akcji wykonywanych w celu ograniczenia wpływu ataku,
   - możliwość zapisywania raportów w formie PDF,
   - możliwość wysyłania raportów w formacie PDF za pomocą email, bezpośrednio z aplikacji,

a. Dostęp do statystyk ruchu przechodzącego przez Usługę (bieżących i historycznych)

b. Dostęp do portalu powinien odbywać się szyfrowanym kanałem HTTPS.

5.2. Raporty miesięczne

Zamawiający wymaga generowania i dostarczania comiesięcznych raportów ochrony przed atakami typu DDoS, zawierających co najmniej następujące statystyki:

a. uśredniony poziom ruchu wchodzącego i wychodzącego,
b. skuteczność Usługi,
c. maksymalne poziomy ruchu wchodzącego i wychodzącego,
d. liczba zarejestrowanych ataków,
e. liczba usuniętych ataków
f. priorytety zarejestrowanych ataków,
g. CRA,
h. CRZ,
i. CRAC.

Raporty te mogą być publikowane w panelu zarządzania Usługą, przy jednoczesnym poinformowaniu Zamawiającego mailem o ich opublikowaniu.

5.3. Raport z incydentu

Zamawiający wymaga każdorazowo po zakończeniu operacji oczyszczania ruchu, po zaistniałym ataku, sporządzenia raportu z incydentu. Raporty z incydentu muszą być generowane wyłącznie dla ataków, których wartość szczytowa przekracza 100Gb/s lub czas trwania ataku jest dłuższy niż 6h.

Raport z incydentu zawierać będzie co najmniej następujące statystyki:

a. rozmiar ataku, liczniki pakietów, Gb/s oraz procent całości ruchu,
b. czas trwania ataku,
c. główne źródła ataku,
d. typ i natura ataku,
e. wdrożone metody eliminacji ataku,
f. geograficzna lokalizacja źródeł ataku,
g. wielkość oczyszczonego ruchu,
h. terminy – w szczególności: początek ataku, powiadomienie, wdrożenie procedur obronnych, zakończenie ataku, przywrócenie normalnej pracy sieci.

Raporty z incydentów mogą być publikowane w panelu zarządzania Usługą, przy jednoczesnym poinformowaniu Zamawiającego mailem o ich gotowości.

6. Wdrożenie Usługi

6.1. Projekt wykonawczy

W ciągu 5 (pięciu) dni roboczych po podpisaniu Umowy na świadczenie Usługi, przy współpracy z Zamawiającym, Wykonawca przygotuje projekt wykonawczy zawierający:

a. opis techniczny integracji Usługi z siecią Zamawiającego, wraz z wytycznymi dotyczącymi zmiany konfiguracji urządzeń Zamawiającego wymaganymi do wdrożenia usługi;
b. opis procedur powiadamiania i eskalacji;
c. testy akceptacyjne;
d. opis procedur obsługi zgłoszeń i raportowania.

Dokument zostanie przedłożony w formie pisemnej lub za pośrednictwem poczty elektronicznej do akceptacji Zamawiającego, który w ciągu 3 (trzech) dni roboczych dokona jego akceptacji lub zgłosi do niego uwagi.

W przypadku zgłoszenia uwag, Wykonawca usunie wskazane przez Zamawiającego braki w ciągu 3 (trzech) dni roboczych od dnia ich zgłoszenia przez Zamawiającego i przedłoży dokument do akceptacji Zamawiającego.

Zaakceptowany przez Zamawiającego dokument będzie podstawą do wdrożenia usługi. Komunikacja na etapie uzgadniania projektu wykonawczego będzie się odbywała pomiędzy upoważnionymi reprezentantami Stron.

6.2. Wdrożenie

Wdrożenie Usługi, realizowane w ciągu 14 (czternastu) dni kalendarzowych od zaakceptowania projektu wykonawczego przez Zamawiającego, obejmie rekonfigurację urządzeń Zamawiającego pod kątem monitorowania ruchu oraz uruchomienia Usługi. Konfigurację w/w urządzeń Zamawiający przeprowadzi we własnym zakresie, zgodnie z wytycznymi opisanymi w projekcie wykonawczym.

Wykonawca zestawi łącza do wskazanej lokalizacji urządzenia Zamawiającego.

6.3. Testy akceptacyjne

Po zakończeniu wdrożenia Zamawiający wraz z Wykonawcą przeprowadzą testy akceptacyjne zgodnie z uzgodnionym projektem wykonawczym i stanowiące test funkcjonalny platformy ochrony przeciwko atakom typu DDoS. Testy uwzględnią weryfikację poprawności wdrożonej konfiguracji.

Po skutecznym przeprowadzeniu testów, o których mowa powyżej, podpisany zostanie protokół odbioru usługi, który będzie oznaczał przyjęcie usługi do eksploatacji.

Za termin uruchomienia usługi przyjęty będzie dzień bezpośrednio następujący po dniu podpisania protokołu odbioru usługi.

Przed wdrożeniem pełnej funkcjonalności Usługi Zamawiający wymaga przeprowadzenia, w okresie tygodnia od terminu uruchomienia usługi, procesu analizy ruchu Zamawiającego. Proces ten polega na kierowaniu ruchu z Internetu do infrastruktury Wykonawcy realizującej Usługę. Ruch podczas tego procesu nie podlega żadnym filtracjom i w sposób niezmieniony kierowany jest do sieci Zamawiającego. Platforma czyszczenia ruchu podczas przedmiotowego procesu nauczania zbiera statystyki, na których podstawie jest w stanie określić parametry algorytmów ochrony (ang. countremeasures) tak, aby w trakcie ataku zachować ruch użytkowników, a odfiltrować ruch ataku.

6.4. Instruktaż

W ramach wynagrodzenia Wykonawcy z tytułu świadczenia Usługi, Wykonawca jest zobowiązany do przeprowadzenia instruktażu podstawowego i zaawansowanego dla osób wskazanych przez Zamawiającego.

Instruktaż podstawowy

Instruktaż podstawowy odbywać się będzie w siedzibie Zamawiającego, instruktaż zaawansowany na terenie Warszawy (w szczególności w siedzibie Zamawiającego). Wykonawca jest zobowiązany dostarczyć materiały instruktażowe w wersji papierowej i elektronicznej, najpóźniej w dniu przeprowadzenia danego instruktażu.

W ciągu 14 dni od zatwierdzenia przez Zamawiającego projektu wykonawczego Wykonawca przeprowadzi w siedzibie Zamawiającego, instruktaż podstawowy w zakresie działania Usługi, obsługi zgłoszeń i raportowania, a w szczególności aspektów dotyczących ochrony przed atakami typu DDoS.

W ramach instruktażu Wykonawca przekaże sposób detekcji ataku oraz sposoby uruchomienia usługi w trybie automatycznym oraz ręcznym, a także dostępne opcje (oraz sposoby ich konfiguracji) dla potrzeb strojenia mechanizmów ochronnych.

W instruktażu wezmą udział pracownicy Zamawiającego lub osoby wskazane przez Zamawiającego.

Instruktaż zaawansowany

Wykonawca przeprowadzi dla maksymalnie czterech osób wskazanych przez Zamawiającego zaawansowany instruktaż obejmujący co najmniej:

- konfigurację systemu,
- administrację systemem,
- ochronę behawioralna DoS
- ochronę przed SYN Flood,
- konfigurację limitów połączeń,
- ochronę HTTP Mitigator,
- ochronę sygnaturową,
- konfigurację wyjątków,
- stanowe listy dostępu,
- zarządzenie pasmem.

Instruktaż zaawansowany, poza formą wykładu, musi zawierać elementy praktyczne wykonywane w udostępnionym przez Wykonawcę środowisku laboratoryjnym, tożsamym z dostarczaną Usługą. Praktyczna część instruktażu będzie realizowana na komputerach dostarczonych przez Zamawiającego. Instruktaż zaawansowany musi zostać zakończony wystawieniem certyfikatu przez autoryzowany ośrodek szkoleniowy lub producenta infrastruktury Wykonawcy świadczącego Usługę.

6.5. Dokumentacja powykonawcza

W ciągu siedmiu dni po podpisaniu protokołu odbioru Wdrożenia Usługi Wykonawca przekaże do Zamawiającego dokumentację Usługi. Dokumentacja obejmie co najmniej:

a. sposoby połączeń pomiędzy infrastrukturą Wykonawcy a siecią Zamawiającego,
b. użytą adresację,
c. zmiany w konfiguracji urządzeń Zamawiającego wraz z opisem,
d. sposoby wyzwalania mechanizmów ochronnych (czyszczenia ruchu).

Nieprzekazanie ww. dokumentacji będzie stanowić dla Zamawiającego powód do wstrzymania płatności za Usługę, do czasu przekazania tej dokumentacji.