

Spis treści

Specyfikacja techniczna (załącznik nr 1 do Umowy)	6
I. Obligatoryjne wymagania dotyczące budowy sieci PIPWAN i jej monitorowania	6
II. Wymagania dotyczące łącz symetrycznych doprowadzonych do lokalizacji Zamawiającego	8
Konfiguracja QoS	11
III. Przełączanie transmisji danych pomiędzy łączem MPLS a łączem Zapasowym i na odwrot	12
IV. System monitoringu sieci PIP WAN	12
Wymagane funkcjonalności systemu monitoringu:	12
V. System centralnego zarządzania urządzeniami bezpieczeństwa (FortiManager) .	13
Interfejsy, dyski	13
Parametry wydajnościowe	13
Funkcje systemu centralnego zarządzania:	13
Zarządzanie	14
Gwarancja i wsparcie	14
VI. Szczegółowa charakterystyka świadczonej usługi	15
A. System ochrony przed atakami wolumetrycznymi DDOS dla łącza internetowego w GIP 15	
W ramach ochrony przed atakami DDoS Wykonawca zapewni:	15
Wykrywanie zagrożeń	16
Mitygacja - oczyszczanie ruchu	16
Poziom SLA dotyczący powiadomienia o ataku DDoS	17
Raporty miesięczne	17
Raport z incydentu	18
Obszar działania Usługi	18
B. System ochrony przed atakami DDOS dla usług internetowych w GIP	18
Architektura systemu	18
System operacyjny	18
Parametry fizyczne systemu	18
Wymagania ogólne	19
Funkcje bezpieczeństwa	19
Zaawansowane mechanizmy bezpieczeństwa	20
Parametry wydajnościowe	21

Zarządzanie, logowanie i raportowanie	21
C. System dostępu i bezpieczeństwa sieci PIP WAN dla GIP i OSPIP - klaster HA...	22
Wymagania ogólne.....	22
Redundancja, monitoring i wykrywanie awarii	23
Interfejsy, dyski, zasilanie.....	23
Parametry wydajnościowe:.....	23
Funkcje Systemu Bezpieczeństwa:	24
Polityki, firewall.....	24
Połączenia VPN	24
Routing i obsługa łączy WAN	25
Zarządzanie pasmem	25
Kontrola Antywirusowa	25
Ochrona przed atakami	26
Kontrola aplikacji	26
Kontrola WWW	26
Optymalizacja i akceleracja połączeń ruchu internetowego	27
Uwierzytelnianie użytkowników w ramach sesji.....	27
Zarządzanie	27
Logowanie	28
Certyfikaty	28
Serwisy i licencje	28
D. System dostępu i bezpieczeństwa sieci dla 16 jednostek OIP: Białystok, Bydgoszcz, Gdańsk, Katowice, Kielce, Kraków, Lublin, Łódź, Olsztyn, Opole, Poznań, Rzeszów, Szczecin, Warszawa, Wrocław, Zielona Góra.	28
Wymagania ogólne.....	28
Redundancja, monitoring i wykrywanie awarii	29
Interfejsy, dyski, zasilanie.....	29
Parametry wydajnościowe.....	30
Funkcje Systemu Bezpieczeństwa	30
Polityki, firewall.....	31
Połączenia VPN	31
Routing i obsługa łączy WAN	31
Zarządzanie pasmem	32
Kontrola Antywirusowa	32
Ochrona przed atakami	32

Kontrola aplikacji	32
Kontrola WWW	33
Uwierzytelnianie użytkowników w ramach sesji.....	33
Zarządzanie.....	33
Logowanie:	34
Certyfikaty	34
Serwisy i licencje	34
E. System dostępu i bezpieczeństwa sieci dla każdej z 44 pozostałych siedzib (OOPIP - 43 i hotel).....	35
Wymagania Ogólne	35
Redundancja, monitoring i wykrywanie awarii	35
Interfejsy, dyski, zasilanie.....	35
Parametry wydajnościowe:.....	36
Funkcje Systemu Bezpieczeństwa	36
Polityki, firewall.....	37
Połączenia VPN	37
Routing i obsługa łącz WAN	37
Zarządzanie pasmem	38
Kontrola Antywirusowa	38
Ochrona przed atakami	38
Kontrola aplikacji	38
Kontrola WWW	39
Uwierzytelnianie użytkowników w ramach sesji.....	39
Zarządzanie.....	39
Logowanie:	40
Certyfikaty	40
Serwisy i licencje	40
VII. Access pointy	41
VIII. System zarządzania bezpieczeństwem stacji roboczych wraz z realizacją dostępu zdalnego VPN	42
Architektura systemu	42
Parametry systemu zarządzania bezpieczeństwem stacji roboczych.....	43
Parametry centralnego systemu zarządzania.....	44
Licencje i serwisy	45
IX. SIEM (Security Information and Event Management) - System analizy i korelacji zdarzeń występujących w sieci PIP WAN	46

Wymagania sprzętowe	46
Wymagania Licencyjne.....	47
Logowanie	47
Zbieranie danych:.....	49
Korelacja Logów	49
Raportowanie	50
Analityka.....	50
Zarządzanie.....	51
X. System ochrony poczty.....	52
Parametry fizyczne systemu antyspamowego.....	52
Ogólne funkcje systemu ochrony poczty	52
Kontrola antyspamowa	53
Ochrona przed atakami na usługę poczty.....	54
Funkcje logowania i raportowania	54
Funkcje pracy w trybie wysokiej dostępności (HA)	55
Aktualizacje sygnatur, dostęp do bazy spamu.....	55
Zarządzanie.....	55
Certyfikaty	55
Serwisy i licencje	55
Gwarancja oraz wsparcie	55
XI. System proaktywnej ochrony przed zaawansowanymi zagrożeniami	56
System operacyjny	56
Parametry fizyczne systemu.....	56
Funkcjonalności podstawowe i uzupełniające	57
Parametry wydajnościowe.....	57
Zarządzanie.....	57
Serwis i usługi	58
Zasilanie	58
XII. Wymagania ogólne Reguły bezpieczeństwa	58
XIII. Opieka serwisowa	59
XIV. Administracja systemem	60
XV. Adresacja publiczna IP	61
XVI. Testy poprawności konfiguracji urządzeń i sieci PIP WAN.....	61
XVII. Wymagania dotyczące szkoleń	61
Wymagania ogólne dotyczące szkoleń.....	61
Minimalny zakres tematyczny szkoleń.....	66

Specyfikacja techniczna (załącznik nr 1 do Umowy)

I. Obligatoryjne wymagania dotyczące budowy sieci PIPWAN i jej monitorowania

Zamawiający ze względu na specyfikę pracy posiadanych i planowanych systemów informatycznych przyjmuje wariant realizacji usługi PIP WAN z wykorzystaniem urządzeń UTM umożliwiających utworzenie 62 węzłów bezpieczeństwa (tj. w każdej lokalizacji PIP umieszczony musi być węzeł bezpieczeństwa). Każdy z węzłów bezpieczeństwa musi posiadać jednakowo wysoki poziom zabezpieczeń. Funkcjonalności bezpieczeństwa uruchomione na każdym węźle muszą umożliwiać kierowanie ruchu do i z Internetu lokalnie. Kontrola i zarządzanie poziomem bezpieczeństwa wszystkich węzłów ma się odbywać zdalnie z jednego centralnego punktu. Ruch aplikacji obejmujący wymianę informacji pomiędzy węzłami musi odbywać się za pośrednictwem kanałów VPN zestawianych na bazie łącz symetrycznych IP VPN MPLS. Transmisja ruchu internetowego w każdej lokalizacji musi być zrealizowana poprzez symetryczne łącza zapasowe. Sieć WAN ma być zbudowana w technologii VPN „full mesh” dla wszystkich jednostek PIP.

Dla wszystkich lokalizacji PIP (GIP, OIP, OOIP i OSPIP) Wykonawca ma zapewnić łącza symetryczne IP VPN MPLS jako łącza podstawowe oraz dodatkowe, zapasowe łącza symetryczne, poprzez które w każdej lokalizacji PIP (lokalnie) będzie realizowany dostęp do Internetu. W przypadku awarii któregośkolwiek z łącz drugie łącze automatycznie przejmie na siebie funkcjonalności łącza uszkodzonego z przeniesieniem całego ruchu na łącze sprawne z utrzymaniem klas ruchu - QoS, Po usunięciu awarii system przełączy się automatycznie na warunki pierwotne. Ponadto Zamawiający wymaga uruchomienia funkcjonalności umożliwiających uporządkowanie ruchu i eliminację zagrożeń pojawiających się w transmisji wewnątrz rozległej komunikacji WAN. Ponadto, w ramach usługi, Zamawiający wymaga:

- uruchomienia i utrzymania sieci WAN w trybie „Client to site” dla 3000 komputerów przenośnych (Wykonawca dostarczy dedykowanego klienta VPN). Usługa ta ma umożliwiać uruchomienie funkcjonalności bezpieczeństwa na komputerach przenośnych, umożliwiając realizację bezpiecznej komunikacji przez Internet bezpośrednio z komputera przenośnego oraz automatyczne zestawienie szyfrowanego kanału VPN do sieci PIP WAN przed zalogowaniem do systemu operacyjnego komputera, filtrowanie stron www, centralne zarządzanie i logowanie zdarzeń.
- uruchomienia dostępu do PIPWAN dla smartfonów i tabletów. (Wykonawca udostępni nielimitowanego klienta VPN). Usługa ta ma umożliwiać bezpieczną komunikację przez Internet bezpośrednio z urządzenia do sieci PIPWAN poprzez zestawienie szyfrowanego kanału VPN.

Zamawiający wymaga, aby zarządzanie urządzeniami (węzłami bezpieczeństwa) odbywało się przez administratora lokalnego (w ramach podległości terytorialnej). Logi pochodzące z urządzeń i oprogramowania zbierane mają być na urządzeniach lokalnych, do których mają dostęp administratorzy lokalni i w GIP na osobnym, wydzielonym urządzeniu umożliwiającym analizowanie i korelację występujących zdarzeń.

W okresie świadczenia usługi całością sieci administrować będzie Wykonawca pod nadzorem Zamawiającego w zakresie konfiguracji, rekonfiguracji, zmiany polityk bezpieczeństwa, zmiany DLP, ustalania QoS (klas ruchu), itp. Zbieranie i archiwizowanie logów wskazanych przez Zamawiającego leży po stronie Wykonawcy. Zamawiający musi posiadać dostęp do logów oraz możliwość eksportu logów. Zamawiający musi posiadać dostęp do systemu monitorowania sieci PIP WAN.

Zadaniem Wykonawcy w ramach świadczenia usługi jest utrzymanie w sprawności łączy, urządzeń klasy UTM, połączeń pomiędzy jednostkami PIP oraz udzielanie wsparcia przy rozwiązywaniu problemów konfiguracyjnych.

Urządzenia UTM muszą być jednocześnie koncentratorami VPN-owymi, które w zależności od typu lokalizacji PIP przyjmą i obsłużą bez uszczerbku dla wydajności jednoczesne połączenia VPN z zewnątrz (klient VPN dostarczony w ramach realizacji usługi). Zestawiony kanał VPN musi umożliwiać pracę z urządzenia przenośnego, tak jakby pracowało w sieci lokalnej lokalizacji do której zestawione jest połączenie VPN.

Zamawiający wymaga, aby urządzenia zaoferowane do stworzenia sieci PIP WAN spełniały wymagania bezpieczeństwa dla każdego węzła i posiadały następujące mechanizmy ochronne:

- Firewall,
- Antywirus (w tym także antymalware),
- AntySPAM,
- IPS,
- DLP,
- Web Filtering,
- Kontrola aplikacji,
- Urządzenia muszą wspierać kodeki dla obsługi VoIP.

1. G.711 - tradycyjna 64-kilobitowa technika kodowania PCM, wykorzystywana w publicznych sieciach telefonicznych,
2. G.729 - kompresja typu CELP, gdzie transmisja głosu przesyłana jest w strumieniu 8 kb/s, zapewniająca wysoką jakość głosu,
3. G.723.1 - część standardu H.324 opisująca dwa sposoby kodowania z wysokim stopniem

kompresji - 5,3 i 6,3 kb/s.

Wszystkie elementy służące do realizacji przedsięwzięcia muszą spełniać wymogi zawarte w europejskim rozporządzeniu o ochronie danych osobowych (RODO).

II. Wymogi dotyczące łączy symetrycznych doprowadzonych do lokalizacji Zamawiającego

Wykonawca doprowadzi do wszystkich siedzib Zamawiającego symetryczne łącza podstawowe IP VPN MPLS i zapasowe z wykorzystaniem jednego z nośników:

- pary kabli miedzianych,
- światłowodu,
- łącza telekomunikacyjnego bezprzewodowego typu punkt-punkt pracującego w paśmie koncesjonowanym,

z zastrzeżeniem, że Zamawiający wymaga, aby:

- łącza podstawowe i zapasowe do lokalizacji GIP, OIP, OSPIP muszą być doprowadzone z wykorzystaniem technologii światłowodowej, poprowadzone dwoma niezależnymi drogami niezależnymi geograficznie bez pojedynczego wspólnego punktu awarii do budynku,
- łącza podstawowe i zapasowe do lokalizacji OOIP muszą być poprowadzone dwoma niezależnymi drogami, niezależnymi geograficznie bez pojedynczego wspólnego punktu awarii do budynku, przy czym łącza podstawowe musi być wykonane w technologii światłowodowej,
- łącza zapasowe nie były zrealizowane za pomocą tego samego fizycznego łącza, na którym zrealizowane będą łącza podstawowe,
- łącza zapasowe, które będzie wykorzystywane jako łącza dostępne do Internetu dla każdej lokalizacji PIP było zrealizowane lokalnie,
- łącza podstawowe i zapasowe muszą być poprowadzone z dwóch niezależnych węzłów operatora,

W celu zapewnienia bezpieczeństwa transmisji danych podstawowe łącza MPLS nie mogą być budowane z wykorzystaniem:

- infrastruktury znajdującej się poza terytorium RP,
- zasobów publicznej sieci Internet,
- łączy asymetrycznych w technologii xDSL,
- łączy satelitarnych,

- łączy w technologii radiowych w paśmie nie podlegającym koncesjonowaniu,
- komutowanych łączy telefonicznych,
- technologii WiFi,
- w oparciu o sieci komórkowe.

Wszystkie prace i roboty budowlane, a także instalacje, w szczególności trasy kablowe, dla każdej lokalizacji, nie mogą obciążać kosztami Zamawiającego.

W celu wykonania instalacji Wykonawca zobowiązany jest dla każdej lokalizacji zdobyć w imieniu Zamawiającego wymagane pozwolenia, decyzje i zgody, w szczególności konserwatora zabytków, oraz wykonać konieczne projekty, roboty budowlane, w tym prace wykończeniowe, porządkowe i inne. Dokumentacja projektowa oraz prace podlegają kontroli i odbiorom przez inspektora nadzoru inwestorskiego.

W przypadku, gdy Wykonawca wykonywał będzie prace do realizacji sieci PIP WAN, w siedzibie gdy jednostka organizacyjna Państwowej Inspekcji Pracy ma siedzibę w budynku, który nie znajduje się w trwałym zarządzie jednostki, a np. jest wynajmowany lub dzierżawiony to kwestia ewentualnej zgody należy i zależy od osoby uprawnionej np. właściciela lub zarządcy, Zamawiający gwarantuje Wykonawcy dostęp do obiektów i pomieszczeń w budynkach, w których Zamawiający wymaga dostarczenia łączy transmisji danych oraz umożliwi wykonywanie prac związanych z uruchomieniem i świadczeniem usług. Ewentualne koszty związane z zamówieniem linii, ich montażem i utrzymaniem w czasie trwania Etapu I i II oraz demontażem po zakończeniu świadczenia usługi zobowiązany jest ponieść Wykonawca.

Łącza telekomunikacyjne na odcinku od węzła Wykonawcy do urządzenia zamontowanego u Zamawiającego nie mogą być wykorzystywane do świadczenia przez Wykonawcę jakichkolwiek usług dla klientów innych niż Zamawiający.

Łącze podstawowe IP VPN MPLS i łącze zapasowe w każdej lokalizacji muszą być łącami bez jakichkolwiek ograniczeń przesyłanych danych oraz łącami symetrycznymi, tj. o jednakowej, minimalnej wskazanej w załączniku nr 2 do umowy Wykaz jednostek organizacyjnych Państwowej Inspekcji Pracy wraz z minimalnymi parametrami łączy w lokalizacjach o szybkości transmisji danych w obu kierunkach.

Wymagane przez Zamawiającego szybkości transmisji danych muszą być gwarantowane przez Wykonawcę jako minimalne szybkości transmisji danych dostępne dla aplikacji Zamawiającego w sieci WAN, dla każdej lokalizacji Zamawiającego, przy założeniu komunikacji z wykorzystaniem protokołów TCP/IP oraz przy założeniu parametru MTU na poziomie 1500 dla transmisji z urządzenia posadowionego u Zamawiającego w stronę routera Wykonawcy i odwrotnie.

Szybkość transmisji danych będzie sprawdzana pomiędzy interfejsem urządzenia posadowionego od strony sieci WAN w jednostkach organizacyjnych Zamawiającego, a urządzeniem posadowionym w każdej lokalizacji. Niedotrzymanie parametru minimalnej gwarantowanej szybkości transmisji danych przez strony Umowy traktowane będzie jako awaria. Metodę pomiaru parametrów łącza Wykonawca przedstawi Zamawiającemu do akceptacji wraz z projektem sieci PIPWAN.

Zamawiający wymaga skonfigurowania priorytetów ruchu na łączy podstawowym MPLS oraz na łączy zapasowym. W tym celu Wykonawca musi oferować dla łączy podstawowych oraz zapasowych usługę QoS. Wartości graniczne parametrów dla poszczególnych klas ruchu QoS dla każdego łącza, pomiędzy lokalizacjami Zamawiającego wskazano w tabeli nr 2, przy czym klasy Voice i Video muszą być typu LLQ (Low Latency Queueing), a klasy Data, Network control i Best effort muszą być typu WFQ (Weighted Fair Queueing) lub CBWFQ (Class Based Weighted Fair Queueing) lub innego równoważnego.

Tabela nr 2

<i>Klasy ruchu QoS</i>	<i>Utrata pakietów</i>	<i>Opóźnienie (RTT)</i>	<i>JITTER</i>
<i>Głos (Voice)</i>	<i><0,1 %</i>	<i>< 40 ms</i>	<i>< 20 ms</i>
<i>Wide (Video)</i>	<i><0,1 %</i>	<i>< 50 ms</i>	<i>< 30 ms</i>
<i>Aplikacje (Data)</i>	<i><0,5%</i>	<i>< 60 ms</i>	
<i>Reszta ruchu (Best effort)</i>	<i>< 1 %</i>	<i>< 100 ms</i>	
<i>Kontrola sieci (NetWork control)</i>	<i><0,5%</i>	<i>< 60 ms</i>	

Utrata pakietów i opóźnienie będą kontrolowane przez Zamawiającego pomiędzy urządzeniami posadowionymi w siedzibach Zamawiającego przez Wykonawcę za pomocą aplikacji ping lub równoważnej przy założeniu, że wielkość wysyłanej paczki danych wynosi: 64 bajty dla klasy Voice, 128 bajtów dla pozostałych klas QoS.

Zamawiający uznaje parametry łącza podstawowego i łącza zapasowego za poprawne jeżeli średnia utrata pakietów oraz średnie opóźnienie za okres minimum pięciu minut nie przekroczy wartości wymienionych w tabeli nr 2. Podział procentowy, w ramach przepustowości łącza, dla każdej z klas ruchu zostanie uzgodniony z Wykonawcą podczas wdrożenia, przy czym wstępnie Zamawiający przyjmuje, że:

- suma gwarantowanych pasm przepustowości poszczególnych klas QoS nie będzie

przekraczać 75 % założonej przepustowości łącza,

- pojedyncza gwarantowana klasa ruchu będzie zajmować do 33% dostępnej przepustowości łącza,
- klasy *Voice* i *Video* będą zajmować łącznie nie więcej niż 40% przepustowości łącza.

Wykonawca musi zapewnić brak pojedynczego punktu awarii jednocześnie dla obu kanałów transmisji, tj. dla łącza podstawowego i zapasowego w każdej lokalizacji Zamawiającego i w swojej infrastrukturze telekomunikacyjnej.

Przez cały czas trwania Etapu I i II, Zamawiający zastrzega sobie możliwość zażądania dostarczenia projektów tras kablowych celem weryfikacji poziomu niezawodności i bezpieczeństwa infrastruktury fizycznej.

Transmisja danych w sieci WAN musi być szyfrowana sprzętowo na poziomie urządzeń posadowionych w lokalizacjach Zamawiającego, a dostarczonych przez Wykonawcę.

Utrata pakietów i opóźnienie dla łącza zapasowego będą kontrolowane przez Zamawiającego, przy wykorzystaniu ping lub aplikacji równoważnej przy założeniu, że wielkość wysyłanej paczki danych wynosi 128 bajtów, przy czym Zamawiający zastrzega sobie prawo do zgłoszenia awarii łącza dla dostępu do Internetu również w przypadku, jeżeli system monitoringu będzie wskazywał, że łącze to nie dotrzymuje wymaganych parametrów. Zamawiający uznaje utratę pakietów oraz opóźnienie dla łącza zapasowego za poprawne jeżeli średnia utrata pakietów oraz średnie opóźnienie za okres minimum pięciu minut nie przekroczy wartości podanych w tabeli nr 3. Parametry te mają być zagwarantowane przez Wykonawcę do punktu styku z siecią Internet .

Tabela nr 3

LOKALIZACJA	Utrata pakietów	Opóźnienie (RTT)
GIP	<0,1 %	< 50 ms
Jednostki organizacyjne PIP	<0,1 %	< 60 ms

Konfiguracja QoS

Zamawiający wymaga, aby w konfiguracji klas ruchu możliwe były przynajmniej następujące ustawienia:

1. skonfigurowanie kolejek typu LLQ dla klas Voice i Video,
2. skonfigurowanie kolejek WFQ lub CBWFQ lub innych równoważnych dla pozostałych klas QoS (z wyjątkiem Best effort),
3. skierowanie całego ruchu do jednej klasy QoS,

4. skierowanie ruchu wydzielonego za pomocą ACL (listy dostępu) do konkretnej klasy QoS, a za pomocą innej ACL do innej klasy QoS,
5. obsługa w ramach jednej klasy QoS ruchu skierowanego za pomocą ACL,
6. skierowanie domyślnego ruchu do klasy Best effort,
7. skierowanie nadmiarowego ruchu w klasie Data lub NetWork control do klasy Best effort.

III. Przełączanie transmisji danych pomiędzy łączem MPLS a łączem Zapasowym i na odwrót

Domyślnie transmisja danych w sieci WAN pomiędzy lokalizacjami Zamawiającego musi odbywać się poprzez podstawowe łącze IP VPN MPLS. W momencie utraty łączności urządzenie UTM w lokalizacji musi, bez zbędnej zwłoki, w sposób automatyczny przełączyć transmisję danych na łącze zapasowe. Po ustaniu awarii transmisja danych musi ponownie, bez zbędnej zwłoki, przełączyć się automatycznie na podstawowe łącze.

Przełączenie transmisji danych w sieci WAN na łącze zapasowe powinno równolegle uruchomić zestaw reguł ACL, dotyczący transmisji danych na łączu zapasowym, który m. in. blokuje określony, mniej istotny ruch w każdej klasie QoS w sieci WAN Zamawiającego.

W wypadku awarii łącza zapasowego musi nastąpić automatyczne przełączenie ruchu internetowego na łącze podstawowe do klasy QoS *Best effort*. Po przywróceniu do pracy łącza zapasowego automatycznie ruch internetowy ma być przekierowany na to łącze i odłączony od podstawowego łącza.

IV. System monitoringu sieci PIP WAN

Zamawiający musi posiadać dostęp do systemu monitorowania sieci PIP WAN. System monitorowania musi posiadać następujące funkcjonalności:

- Wykonawca udostępni i uruchomi dynamiczne (pracujące w czasie rzeczywistym) wyświetlanie mapy logicznej i fizycznej topologii sieci PIP WAN z urządzeniem brzegowym Wykonawcy w każdej lokalizacji włącznie,
- weryfikację statusu każdego łącza podstawowego MPLS, tj. czy łącze jest aktywne, czy uległo awarii, oraz rejestrowanie zmiany aktywności,
- weryfikację statusu każdego łącza zapasowego, tj. czy łącze jest aktywne czy uległo awarii, oraz rejestrowanie zmiany aktywności.

Wymagane funkcjonalności systemu monitoringu:

1. zbieranie danych z urządzeń brzegowych wykonawcy.
2. możliwość przechowywania pełnych danych przez okres minimum roku.

3. dostęp do wszystkich zebranych danych oraz raportów za pośrednictwem przeglądarki WWW dla administratorów z lokalizacji GIP, OSPIP, OIP.
4. możliwość bezpośredniego eksportowania danych i raportów.
5. możliwość automatycznego generowania, zapisywania i wysyłania raportów pocztą email.

V. System centralnego zarządzania urządzeniami bezpieczeństwa

W ramach realizacji przedmiotu zamówienia Wykonawca musi dostarczyć system centralnego zarządzania przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW). Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Interfejsy, dyski

1. System musi dysponować co najmniej 4 portami Gigabit Ethernet RJ-45, oraz portem konsoli szeregowej.
2. Powierzchnia dyskowa min, 6 TB.
3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika - minimum RAID 1, 5, 10.

Parametry wydajnościowe

System musi umożliwiać zarządzanie co najmniej 100 systemami bezpieczeństwa.

Funkcje systemu centralnego zarządzania:

W ramach centralnego systemu zarządzania muszą być realizowane co najmniej poniższe funkcje:

1. System musi posiadać system zarządzania zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3. System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4. System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5. System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.

6. System musi umożliwiać zarządzanie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.
7. System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8. System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach posadowionych w lokalizacjach Zamawiającego oraz zdalnymi uaktualnieniami.
10. System musi monitorować i zapisywać w czasie rzeczywistym zdalne wykonywanie skryptów na urządzeniach posadowionych w lokalizacjach Zamawiającego.
11. System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).
12. System musi automatyzować proces konfiguracji struktur VPN typu Hub-and-Spoke
13. oraz Full-Mesh.
14. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów; HTTPS oraz SSH.
2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
3. System musi posiadać API które umożliwia zarządzanie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.

Gwarancja i wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym przez cały okres trwania Etapu II, polegającym na naprawie lub wymianie urządzenia w przypadku awarii lub jego wadliwości. W ramach tego serwisu musi zostać zapewniony również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w dniach roboczych i godzinach roboczych.

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy w ciągu 9 godzin roboczych od przekazania zgłoszenia przez Zamawiającego.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim siedem dni w tygodniu, 24 godziny na dobę przez dedykowany

serwisowy moduł internetowy oraz infolinię w języku polskim siedem dni w tygodniu, 24 godziny na dobę.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszej Umowy (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć w I etapie realizacji Umowy 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. 2020 poz.509 t.j.) 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.

VI. Szczegółowa charakterystyka świadczonej usługi

Podane parametry dla urządzeń zabezpieczających są parametrami minimalnymi.

Zamawiający dopuszcza zastosowanie systemu składającego się z kilku urządzeń.

Wielkość rozwiązania zaproponowanego przez Wykonawcę nie może przekraczać dla rozwiązania zainstalowanego w:

- GIP - Głównym Inspektoracie Pracy GIP - max 20U.
- OSPIP - Ośrodkiem Szkolenia Państwowej Inspekcji Pracy OSPIP- max. 8U,
- OIP - Okręgowym Inspektoracie Pracy OIP - max. 4U,
- OOIP - Oddziale Okręgowego Inspektoratu Pracy OOIP- max. 2U,

Zaoferowane urządzenia muszą wspierać telefonię VoIP. System musi wspierać, co najmniej protokoły SIP, H323, RTP, SCCP. System musi wspierać funkcje ochrony IPS, co najmniej dla protokołu SIP. System musi wspierać Application Level Gateway dla SIP (SIP ALG).

A. System ochrony przed atakami wolumetrycznymi DDOS dla łącza internetowego w GIP

W ramach ochrony przed atakami DDoS Wykonawca zapewni:

1. analizę ruchu w celu identyfikacji typu i natury ataku,
2. powiadamiania Zamawiającego o podejrzeniu wystąpienia ataku,
3. rozpoczęciu usuwania ataku w porozumieniu z Zamawiającym (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia),
4. modyfikację zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny

poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy,

5. klasyfikacji alarmów typu DDoS jako:

- a) zweryfikowany atak,
- b) fałszywy alarm,
- c) nagły ruch – znaczący wzrost ruchu, spowodowany inną przyczyną niż atak na daną usługę Zamawiającego.

Wykrywanie zagrożeń

1. Wykonawca zapewnienia efektywną identyfikację potencjalnych ataków DDoS z wykorzystaniem poniższych mechanizmów detekcji:
 - a) sygnatury,
 - b) przekroczenie progów dla określonych typów pakietów i protokołów,
 - c) opartych na analizie profilu ruchu Zamawiającego wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu.
2. Usługa monitoruje ruch do i od chronionej podsieci w czasie rzeczywistym, w tym w odniesieniu do poszczególnych usług Zamawiającego. Lista usług Zamawiającego realizowanych na udostępnionym łączu, jest listą otwartą i może się zmieniać z dnia na dzień w okresie realizacji Umowy, w zależności od uruchamianych / kasowanych usług Zamawiającego.
3. Usługa zapewnia wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu internetowym, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS TCP SYN.
4. System realizujący usługę na podstawie danych historycznych wyznacza oczekiwaną wartość ruchu do i od chronionej podsieci o danej porze dnia w danym dniu tygodnia, w odniesieniu do poszczególnych usług Zamawiającego.
5. Usługa zapewnia wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu oraz wykrywanie potencjalnych Ataków w warstwie transportowej (warstwa 4 modelu OSI) dla poszczególnych usług Zamawiającego w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu.

Mitygacja – oczyszczanie ruchu

1. Wykonawca zapewnia wykonanie usługi ochrony przed atakami DDoS, polegającej na usuwaniu ataku przy możliwie jak najmniejszym wpływie na ruch uprawniony. Efektywne działanie powinno obejmować trzy procedury:
 - a) procedura uruchamiana w przypadku podejrzenia wystąpienia ataku: ruch

przekierowany zostanie do dedykowanych do tego celu zasobów wewnętrznych

Wykonawcy,

- b) procedura filtrowania, oparta o wielowarstwową analizę ruchu i mechanizmy przeciwdziałania,
- c) procedura oparta o kierowanie odfiltrowanego ruchu z powrotem do Zamawiającego.

2. Wykonawca zapewnia ochronę co najmniej przed następującymi typami ataków:

- a) TCP SYN flood
- b) UDP flood (w tym DNS reflection)
- c) HTTP GET flood
- d) HTTP POST flood
- e) ICMP flood
- f) IGMP flood
- g) invalid packets
- h) IP fragments
- i) IP NULL
- j) DNS flood
- k) SIP request flood
- l) SSL negotiation

Poziom SLA dotyczący powiadomienia o ataku DDoS

1. Czas Reakcji na atak DDoS (CRA) maksymalnie 15 minut. Przez CRA rozumie się czas, jaki upłynie od wykrycia ataku DDoS do rozpoczęcia skutecznego poinformowania Zamawiającego, za pośrednictwem poczty elektronicznej, z zastrzeżeniem, że dopuszcza się formę telefoniczną w przypadku braku możliwości przesłania informacji poprzez pocztę elektroniczną
2. Czas Reakcji na Zlecenie oczyszczania ruchu (CRZ) maksymalnie 15 minut. Przez CRZ rozumie się czas, jaki upłynie od przyjęcia Zlecenia od Zamawiającego z żądaniem włączenia lub wyłączenia oczyszczania po zarejestrowanym ataku DDoS.

Raporty miesięczne

Wykonawca umieszcza w comiesięcznych raporcie dotyczącym usługi ochrony przed atakami DDoS informację zawierającą następujące statystyki:

1. uśredniony poziom ruchu wchodzącego i wychodzącego,
2. maksymalne poziomy ruchu,
3. liczba zarejestrowanych ataków DDoS,

4. liczba usuniętych ataków DDoS.

Raport z incydentu

Wykonawca każdorazowo po zakończeniu operacji oczyszczania ruchu po zaistniałym ataku DDoS sporządzi raportu z incydentu w terminie 5 dni od zamknięcia incydentu. Informacja w raporcie o incydencie zawiera następujące statystyki:

1. rozmiar ataku, liczniki pakietów, Gb/s oraz procent całości ruchu,
2. czas trwania ataku,
3. główne źródła ataku,
4. typ i natura ataku,
5. wdrożone metody eliminacji ataku,
6. geograficzna lokalizacja źródeł ataku,
7. wielkość oczyszczonego ruchu,
8. czasy – w szczególności: początek ataku, powiadomienie, wdrożenie procedur obronnych, zakończenie ataku, przywrócenie normalnej pracy sieci.

Obszar działania Usługi

Wykonawca zapewni, iż ruch w sieci Zamawiającego przekierowany do oczyszczania jest wysyłany wyłącznie na obszar znajdujący się pod bezpośrednim nadzorem Wykonawcy na terenie Polski.

B. System ochrony przed atakami DDOS dla usług internetowych w GIP

Architektura systemu

Dla zapewnienia bezpieczeństwa i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta i były realizowane w obrębie pojedynczego urządzenia sieciowego.

System operacyjny

Zamawiający wymaga aby dostarczone urządzenia sieciowe pracowało w oparciu o dedykowany system operacyjny.

Parametry fizyczne systemu

- Minimum 8 interfejsów 1GE RJ-45,
- w tym 4 pary interfejsów z wbudowaną funkcją bypass,
- Minimum 4 interfejsy 1GE SFP,
- Minimum 4 interfejsy LC SR GE z wbudowaną funkcją bypass,
- Minimum 1 port USB,

- dysk w technologii SSD o pojemności minimum 480GB,
- redundantny, wbudowany zasilacz,
- urządzenie musi mieć możliwość montowania standardowej szafie teletechnicznej 19 calowej,
- urządzenie nie może zajmować wysokości większej niż 1U,

Wymagania ogólne

System powinien pozwalać na nie mniej niż:

- inspekcji transparentny „bridge” - brak konieczności ingerencji w adresację IP,
- inspekcja w trybie inline nie może powodować modyfikacji adresacji MAC i/lub IP analizowanych ramek,
- wsparcie dla analizy ruchu VLAN (bez konieczności definiowania konkretnych VLAN) także wraz z Q-in-Q,
- możliwość konfiguracji urządzeń w klaster HA Active-Passive,
- analizę, detekcję i ochronę dla ruchu IPv4 oraz IPv6,
- dynamiczne wykrywanie ataków bez konieczności ręcznej kontroli/przekierowania ruchu,
- wykrywanie i ochrona przed atakami zarówno dla ruchu przychodzącego jak i wychodzącego. Wszelkie metody wykrywania i ochrony powinny być możliwe dla każdego z wymienionych kierunków ruchu, a także powinny być wzajemnie od siebie niezależne opierając się na indywidualnych kryteriach i parametrach,
- możliwość wykorzystania trybu automatycznego uczenia celem łatwej identyfikacji wzorców ruchu i komunikacji sieciowej noszącej znamiona anomalii i/lub ataku. Tryb uczenia urządzenia powinien dawać możliwość nauczania i konwersji do zalecanej konfiguracji wszystkich obserwowanych parametrów.

Funkcje bezpieczeństwa

Zadaniem systemu ochrony przed atakami DDoS jest spełnienie następujących wymagań:

- identyfikacja następujących rodzajów ataków/deformacji pakietów: Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number,
- ochrona przed atakami typu low-and-slow. Odrzucanie/przerywanie nieaktywnych sesji TCP w sytuacji gdy określona przez administratora liczba danych (bajtów) nie zostanie przesłana w określonym czasie,

- ograniczanie liczby jednoczesnych połączeń TCP od jednego klienta,
- ochrona przed atakami DDoS dla protokołu SSL/TLS bez konieczności poddawania inspekcji tego rodzaju ruchu,
- zmiana parametrów ochronnych w trakcie działania samych mechanizmów ochronnych. Zmiana nie może powodować przerwy w transmisji,
- zaimplementowane mechanizmy inspekcji i ochrony dla warstw 3, 4 oraz 7 modelu OSI/ISO,
- monitorowanie i ochrona protokołów w warstwie 3 modelu OSI/ISO.: IP(IPv4, IPv6), IPX, ICMP, IGMP, IPsec.
- monitorowanie i ochrona 65 tysięcy portów TCP oraz UDP, wraz z możliwością przedstawienia poziomów ruchu i ilości odrzuconych pakietów dla danego portu,
- system nie może wykorzystywać ani mieć zaimplementowanej obsługi sygnatur celem ochrony przed atakami DDoS . Cały zakres ochrony musi być realizowany tylko i wyłącznie w oparciu o mechanizmy behawioralne (network behavior analysis) i heurystyczne. Rolę wspomagającą mogą mieć mechanizmy reputacyjne.

Zaawansowane mechanizmy bezpieczeństwa

1. System musi wspierać następujące mechanizmy wykrywania i blokowania zagrożeń/ataków:
 - a) TCP Floods,
 - b) UDP Floods,
 - c) Connection Floods,
 - d) Excessive URL/source/second,
 - e) SYN, ACK, RST, FIN Floods,
 - f) Zombie Floods,
 - g) ICMP Floods,
 - h) Fragment Flood,
 - i) HTTP GET Flood,
 - j) Floods from Unwanted Geographical Areas.
2. System musi obsługiwać:
 - a) listy reputacyjne IP,

- b) definicje: adresacji sieci, protokołów, portów TCP/UDP, ICMP, (różne rodzaje pakietów), adresy URL, hostów, odnośników przeglądarek bez konieczności stosowania wyrażeń regularnych,
- c) system musi wykrywać i blokować ataki typu:
 - HTTP flood w metodach: POST, HEAD, OPTIONS, TRACE, PUT, DELETE, CONNECT
 - HTTP URL flood,
 - User Agent flood,
 - Referrer flood,
 - Cookie flood,
 - Host flood,
- d) ochrona przed atakami dotyczącymi ruchu DNS:
 - DNS header anomaly
 - DNS response cache under flood
 - DNS query flood
 - DNS unexpected query
 - DNS query-response matching
 - Unsolicited DNS response flood
 - DNS query flood per source z określonym TTL

Parametry wydajnościowe

Urządzenie musi obsługiwać co najmniej:

- przepustowość minimum 6 Gbps (pakiety 64 bajtowe)
- zdolność do analizy pakietów na poziomie minimum 8 Mpps
- minimum 8 indywidualnych profili bezpieczeństwa
- opóźnienia przy analizie ruchu produkcyjnego na poziomie poniżej 70 mikrosekund
- czas reakcji na atak (ochrony) poniżej 2 sekund

Zarządzanie, logowanie i raportowanie

System musi zapewniać:

- graficzny interfejs zarządzający przy użyciu szyfrowanego połączenia (HTTPS)
- zarządzanie poprzez linię poleceń z wykorzystaniem protokołu SSH bądź też portu szeregowego RS-232
- dedykowany interfejs zarządzający (RJ45) nie będący w ścieżce ruchu produkcyjnego (out-of-band management).

- wbudowany mechanizm pozwalający na tworzenie raportów z horyzontem czasowym nie mniejszym niż 1 rok
- generowanie raportów w następujących formatach: HTML/MHT, PDF, MS Word oraz tekstowy
- możliwość przechowywania raportów lokalnie na urządzeniu lub wysłania mailem bezpośrednio z urządzenia
- wsparcie dla syslog, SNMP oraz REST API

C. System dostępu i bezpieczeństwa sieci PIP WAN dla GIP i OSPIP - klaster HA

Zamawiający wymaga dostarczenia i zainstalowania dwóch niezależnych klastrów (2x2szt = 4 szt. urządzenia bezpieczeństwa i 2x2szt = 4 szt. switch), z których jeden będzie w GIP a drugi w OSPIP. Zamawiający wymaga dostarczenia i zainstalowania w GIP i OSPIP systemu dostępu i ochrony sieci o następujących funkcjonalnościach: firewall, antywirus, antyspam, IPS, web filter, kontrola aplikacji, kontrolę treści (Data Leak Prevention), optymalizacja WAN, możliwość zestawienia tuneli VPN IPsec, oraz kontrola ruchu SSL o parametrach nie gorszych niż zapisane poniżej.

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 Wykonawca musi zapewnić niezbędne do pracy dostarczonych aplikacji platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i dowolnym wirtualizatorem jeżeli dla przyjętego rozwiązania jest wymagany.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewalla, IPSec, VPN, antywirusa, IPS, kontrola aplikacji. Powinna istnieć możliwość dedykowania co najmniej 9 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

Dostarczony system musi zapewniać:

1. W przypadku systemu pełniącego funkcje: firewall, IPSec, kontrola aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy.
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, zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum:
 - a) 2 portami Gigabit Ethernet RJ-45 do zarządzania,
 - b) 16 portami Gigabit Ethernet RJ-45,
 - c) 8 gniazdami Gigabit Ethernet SFP,
 - d) 12 gniazdami 25GE SFP28/ 10GE SFP+/ GE SFP,
 - e) 4 gniazdami 100GE QSFP28.
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 1 TB.
5. System realizujący funkcję Firewall musi być wyposażony co najmniej w podwójny zasilacz.

Parametry wydajnościowe:

1. W zakresie Firewalla obsługa nie mniej niż 12 mln jednoczesnych połączeń oraz 750 000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 189 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 32 Gbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA256: nie mniej niż 52 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 20 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 15 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 11 Gbps.

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 wraz z obowiązkiem dostarczenia przez Wykonawcę niezbędnego sprzętu do obsługi platformy:

1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zapytań DNS.
8. Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Uwierzytelnianie z wykorzystaniem minimum loginu i hasła.

Polityki, firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać NAT źródłowy i docelowy, PAT oraz:
 - translację jeden do jeden oraz jeden do wielu,
 - dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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 algorytmem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Modę (GCM),
 - Obsługa protokołu Diffiego-Hellmana grup 19 i 20,
 - Wsparcie dla pracy w topologii Hub and Spoke oraz Full Mesh,
 - 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,
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać 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 zestawienie tunelu VPN pomiędzy stacją roboczą a urządzeniem bezpieczeństwa.

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, 7-zip.

3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną).

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. System musi posiadać mechanizmy ochrony dla aplikacji Web-owych na poziomie sygnaturowym (co najmniej ochrona przed: XSS (Cross-site scripting), SQL Injecton, trojany, exploity oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, cookies).
6. System musi wykrywać i blokować komunikację C&C do sieci botnet.

Kontrola aplikacji

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

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google.
6. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
7. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Optymalizacja i akceleracja połączeń ruchu internetowego

Urządzenia muszą mieć możliwość uruchomienia funkcjonalności proxy dla ruchu do sieci Internet.

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,
 - statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
 - dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania zdalnego 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. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
4. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
5. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania zdarzeń do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach Umowy musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej wraz z dostarczonym niezbędnym sprzętem/oprogramowaniem do obsługi ww. platformy.
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 IPSec VPN,
- ICSA dla funkcji SSL VPN,

lub równoważne do powyższych.

Serwisy i licencje

W ramach realizacji przedmiotu zamówienia wykonawca musi dostarczyć Zamawiającemu licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrolę aplikacji, IPS, antywirus, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen przez cały okres trwania Etapu II.

D. System dostępu i bezpieczeństwa sieci dla 16 jednostek OIP: Białystok, Bydgoszcz, Gdańsk, Katowice, Kielce, Kraków, Lublin, Łódź, Olsztyn, Opole, Poznań, Rzeszów, Szczecin, Warszawa, Wrocław, Zielona Góra.

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 Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i dowolnym wirtualizatorem, jeżeli dla przyjętego rozwiązania jest wymagany.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewalla, PSec, VPN, antywirus, IPS, kontrola aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

Dostarczony system musi zapewniać:

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

Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, dyski, zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum:
 - 8 portami Gigabit Ethernet RJ-45,
 - 8 portami 5GE RJ-45 lub szybsze,
 - 8 portami 10GE SFP+/SFP,
 - 4 portami 1GE SFP,
 - 2 porty 1 GE RJ45 dedykowane do celów zarządzania lub budowy wysokiej dostępności.
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 co najmniej w podwójny zasilacz.

Parametry wydajnościowe

1. W zakresie Firewalla obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 37 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA256: nie mniej niż 35 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 6 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 5 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 6 Gbps.

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 wraz z obowiązkiem dostarczenia przez Wykonawcę niezbędnego sprzętu do obsługi platformy:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zapytań DNS .
8. Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Uwierzytelnianie z wykorzystaniem minimum loginu i hasła.

Polityki, firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu,
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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,
 - 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.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN, W zakresie tej funkcji musi zapewniać 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 zestawienie tunelu VPN pomiędzy stacją roboczą a urządzeniem bezpieczeństwa.

Routing i obsługa łączy WAN

1. W zakresie routing u 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) łącz 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, 7-zip.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną).

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. System musi posiadać mechanizmy ochrony dla aplikacji Web-owych na poziomie sygnaturowym (co najmniej ochrona przed: XSS (Cross-site scripting), SQL Injecton, trojany, exploity oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, cookies).
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox, Azure) powinny być

kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą haseł:
 - statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
 - statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
 - dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

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. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
4. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
5. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania zdarzeń do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach Umowy musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej wraz z dostarczonym niezbędnym sprzętem/oprogramowaniem do obsługi ww. platformy.
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 IPSec VPN,
- ICSA dla funkcji SSL VPN,

lub równoważne do powyższych.

Serwisy i licencje

W ramach realizacji przedmiotu zamówienia wykonawca musi dostarczyć Zamawiającemu licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrolę aplikacji, IPS, antywirus, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen przez cały okres trwania Etapu II.

E. System dostępu i bezpieczeństwa sieci dla każdej z 44 pozostałych siedzib (OOPIP - 43 i hotel)

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 Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym i dowolnym wirtualizatorem, jeżeli dla przyjętego rozwiązania jest wymagany.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewalla, PSec, VPN, antywirus, IPS, kontrola aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewalla,
- Ochrony w warstwie aplikacji,
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

Dostarczony system musi zapewniać:

1. W przypadku systemu pełniącego funkcje: firewall, IPSec, kontrola aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz 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, zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum:
 - 10 portami Gigabit Ethernet RJ-45.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w dodatkowy zasilacz lub listwę hotswap umożliwiającą automatyczne przełączenie zasilania z minimum dwóch źródeł zasilania.

Parametry wydajnościowe:

1. W zakresie Firewalla obsługa nie mniej niż 1,4 mln jednoczesnych połączeń oraz 34 000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,5 Gbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA256: nie mniej niż 5 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 1,3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej dla ruchu http - minimum 700 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 wraz z obowiązkiem dostarczenia przez Wykonawcę niezbędnego sprzętu do obsługi platformy:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Zarządzanie pasmem (QoS, Traffic shaping).
5. Ochrona przed malware.
6. Inspekcja minimum: IPS ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
7. Kontrola stron WWW.

8. Uwierzytelnianie z wykorzystaniem minimum loginu i hasła.

Polityki, firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać NAT źródłowy i docelowy, PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu,
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

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 algorytmem 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.
 - 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.

Routing i obsługa łącz WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
 - Routingu statycznego,
 - Policy Based Routing,
 - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łącz 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, 7-zip.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną).

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. System musi posiadać mechanizmy ochrony dla aplikacji Web-owych na poziomie sygnaturowym (co najmniej ochrona przed: XSS (Cross-site scripting), SQL Injecton, trojany, exploity oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, cookies).
6. System musi wykrywać i blokować komunikację C&C do sieci botnet.

Kontrola aplikacji

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

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

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

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą haseł:
 - statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
 - statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
 - dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania zdalnego 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. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów

Netflow lub sFlow.

4. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
5. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania zdarzeń do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach Umowy musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej wraz z dostarczonym niezbędnym sprzętem/oprogramowaniem do obsługi ww. platformy.
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 IPSec VPN
- ICSA dla funkcji SSL VPN

lub równoważne dla powyższych.

Serwisy i licencje

W ramach realizacji przedmiotu zamówienia wykonawca musi dostarczyć Zamawiającemu licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrolę aplikacji, IPS, antywirus, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen przez cały okres trwania Etapu II.

VII. Access pointy

1. Wykonawca w ramach realizacji zamówienia musi dostarczyć 33 szt. access pointów, po dwie sztuki do OIP Bydgoszcz, Gdańsk, Katowice, Kraków, Lublin, Łódź, Olsztyn, Opole, Poznań, Rzeszów, Szczecin, Wrocław, Zielona Góra; po jednej sztuce do OIP Białystok, Kielce, Warszawa i 4 szt. do GIP. Zamawiający oczekuje dostawy takich urządzeń oraz ich skonfigurowania, ale nie oczekuje ich fizycznego montażu. Montaż zostanie wykonany przez pracowników Zamawiającego w poszczególnych lokalizacjach, w większości będą to sale konferencyjne. Zamawiający nie wymaga wykonania wizji lokalnych czy pomiarów propagacji sygnałów w poszczególnych lokalizacjach. Zamawiający wymaga skonfigurowania bezpiecznego dostępu do Internetu dla gości oraz dostępu do sieci PIP WAN i Internetu dla pracowników Zamawiającego. Szczegóły dotyczące samej konfiguracji sieci bezprzewodowej, zostaną określone przez Wykonawcę w projekcie sieci PIP WAN.
2. Zamawiający oczekuje, że w ramach Umowy Wykonawca dostarczy system pełniący funkcję kontrolera sieci bezprzewodowych, który zarządza centralnie urządzeniami typu Access Point. Kontroler musi być zrealizowany w postaci funkcjonalności dostarczonej platformy bezpieczeństwa, lub komercyjnej platformy sprzętowej, lub platformy wirtualnej instalowanej na komercyjnych hypervisorach takich jak na przykład VMware, KVM. System nie powinien wymagać dodatkowych licencji na liczbę stacji klienckich. Wykonawca powinien uwzględnić w wycenie dostarczenie zasilaczy POE/POE+ dostosowanych do zaoferowanych urządzeń Access Point. Zamawiający nie wymaga fizycznej instalacji urządzeń Access Point w poszczególnych lokalizacjach. W przypadku awarii urządzenia Access Point Zamawiający własnymi siłami dokona demontażu urządzenia.
3. Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
4. Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na suficie wewnątrz budynku.
5. Urządzenie musi być wyposażone w niezależne moduły radiowe obsługujące następujące standardy:
 - 2.4 GHz 802.11b/g/n,
 - 5 GHz 802.11a/n/ac/ax,
 - 5/6 GHz 802.11a/n/ac/ax
6. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
7. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 100/1000/2500/5000 Base-TX.

8. Zasilane urządzenia poprzez interfejs ETH w standardzie 802.3bt lub zewnętrzny zasilacz.
9. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - Tunnel,
 - Bridge,
 - Mesh.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
 - Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - MIMO – 4x4,
 - Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:
 - 1147 Mbps;
 - 2402 Mbps;
 - 4803 Mbps
 - Wymagana moc nadawania:
 - min. 26 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - min. 26 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - min. 24 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
 - Wsparcie dla 802.11n 20/40Mhz HT,
 - Wsparcie dla kanałów 80 i 160 MHz,
 - Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 6dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.
 - Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
 - Maksymalna deklarowana liczba klientów na każdy moduł radiowy: 512.
11. Urządzenie musi mieć zapewnioną gwarancję producenta przez cały okres trwania Etapu II.

VIII. System zarządzania bezpieczeństwem komputerów przenośnych wraz z realizacją dostępu zdalnego VPN

Architektura systemu

Oferowane rozwiązanie musi pozwalać na centralne zarządzanie komputerami przenośnymi.

Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.

Parametry systemu zarządzania bezpieczeństwem stacji roboczych

Elementy systemu zarządzania dostępem dla stacji roboczych muszą zawierać następujące funkcje i mechanizmy:

- **Kategoryzacja URL**
 - URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków,
 - Możliwość integracji z wtyczką do przeglądarki internetowej, celem analizy kategorii WWW dla ruchu SSL/HTTPS,
- **Analiza podatności**
 - Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
- **Dostęp VPN**
 - Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o aplikacje, przykładowo musi istnieć możliwość wykluczenia aplikacji wymagających dużej ilości pasma np.: Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting, Zoom, WebEx.
 - Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o domeny (FQDN)
 - Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
 - Mechanizmy uwierzytelniania dwuskładnikowego.
 - System musi umożliwiać zastosowanie protokołu SAML dla SSL VPN
 - Możliwość automatycznego zestawiania połączeń VPN (bez interakcji użytkownika),
 - Mechanizm wyboru optymalnego koncentratora VPN w oparciu o czas odpowiedzi serwera oraz TCP Round Trip Time,

- Możliwość zablokowania komunikacji hosta z usługami w ramach sieci LAN oraz Internet do czasu zestawienia połączenia VPN.
- Realizacja bezpiecznych połączeń do usług chronionych NGFW w oparciu o mechanizm pośrednika (proxy), dzięki niewidocznemu dla użytkownika przekierowaniu ruchu do hosta docelowego przez bramę proxy NGFW.
- Oznaczanie stacji roboczych znacznikami TAG, przekazywanymi do rozwiązania NGFW celem wykorzystywania w filtrowaniu ruchu w ramach mechanizmów bezpieczeństwa.
- Mechanizm determinowania czy stacja robocza znajduje się w wewnętrznej sieci chronionej czy poza nią.
- Mechanizmy muszą być dostępne dla następujących wersji systemów operacyjnych Windows: Microsoft Windows 10 (32-bit i 64-bit), Windows 11 (64-bit).

Parametry centralnego systemu zarządzania

- Elementy wchodzące w skład systemu muszą być realizowane w postaci usługi realizowanej w chmurze producenta realizowana na EOG.
- System musi umożliwiać automatyczną aktualizację oprogramowania na komputerach przenośnych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej z urządzeniami NGFW,
- System musi umożliwiać integrację z systemami zarządzania tożsamością użytkowników Active Directory,
- System musi umożliwiać definiowanie różnych profili (wersji konfiguracji) dla różnych grup użytkowników pobieranych z Active Directory lub definiowanych lokalnie,
- System umożliwia przygotowywanie pakietów instalacyjnych przynajmniej dla systemu Windows 32/64 bit, w których administrator może określić komponenty dla instalatora dla komputerów przenośnych takich jak : filtrowanie URL, analiza podatności, agent tożsamości współpracujący z centralnym serwerem uwierzytelniania (SSO),
- Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,
- System musi posiadać możliwość wyświetlania wyników analizy podatności na komputerach przenośnych,
- System musi umożliwiać wyświetlanie w konsoli zarządzania informacji o komputerach przenośnych, które mogą służyć do diagnozy problemów oraz stanu koputera min:
 - Typ połączenia (Ethernet/Wifi),
 - Adres IP,

- Adres IP domyślnej bramy,
- Adres MAC,
- Adres MAC bramy sieciowej,
- Nazwa sieci WiFi (SSID),
- Model sprzętu,
- Producent sprzętu,
- Informacje o procesorze,
- Informacje o pamięci RAM,
- Numer seryjny,
- Informacje o dysku twardym,
- System musi umożliwiać zarządzanie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN,
- Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne,
- System musi udostępniać interfejs API.

Licencje i serwisy

System musi umożliwiać zainstalowanie i centralne zarządzanie minimum 3000 aplikacjami klienckimi zlokalizowanymi na komputerach przenośnych.

W ramach realizacji przedmiotu zamówienia wykonawca musi dostarczyć Zamawiającemu licencje które powinny obejmować cały okres trwania Etapu II.

Dla wskazanej powyżej liczby stacji roboczych licencje muszą zawierać następujące funkcjonalności:

- Filtrowanie adresów URL
- Możliwość zarządzania stacjami roboczymi i profilami SSL VPN i IPSec VPN
- Możliwość wykonywania analizy podatności systemów operacyjnych i zainstalowanych aplikacji
- Centralne zarządzanie
- Centralne logowanie i raportowanie
- Wsparcie dla uwierzytelniania wieloskładnikowego
- Komponentu/agenta pozwalającego na wysyłanie informacji o aktualnie zalogowanym

użytkownika w ramach infrastruktury AD, pozwalającej na budowę transparentnego mechanizmu Single Sign On.

IX. SIEM (Security Information and Event Management) - System analizy i korelacji zdarzeń występujących w sieci PIP WAN

W ramach Umowy wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń PIP WAN oraz dodatkowo musi wspierać obsługę aplikacji typu agent na systemy Windows i Linux.

Rozwiązanie musi być dostarczone tylko w postaci rozwiązań wirtualnych z możliwością migracji/instalacji na platformach sprzętowych również pochodzących od tego samego producenta urządzeń bezpieczeństwa.

Wymagania sprzętowe

Dostarczona platforma sprzętowa musi spełniać następujące wymagania:

1. Serwer wraz z akcesoriami do montażu w standardowej szafie technicznej o szerokości szyn 19 cali.
2. Maksymalna wysokość serwera to 2U.
3. Dwa procesory o minimalnych parametrach 2.4 GHz, 16 rdzeni/32 wątki, 24 MB cache.
4. Minimum 128GB pamięci operacyjnej minimum DDR4, ECC
5. Minimum dwa dyski SSD klasy Read Intensive tworzące RAID0. Dyski muszą mieć możliwość wymiany w czasie pracy.
6. Minimum 8 dysków SATA 6 Gb/s o pojemności co najmniej 8TB, które będą tworzyć grupę RAID6. Dyski muszą mieć możliwość wymiany w czasie pracy.
7. Kontroler zdalnego zarządzania wraz z licencją na połączenia zdalnej konsoli. Dedykowany port sieciowy dla komunikacji zarządzającej serwerem.
8. Karty sieciowe o interfejsach minimum: 2x1Gb RJ45 oraz 2x10Gb SFP+ wraz z wkładkami.
9. Redundantne zasilacze typu hot-swap.
10. Gwarancja producenta na cały okres etapu drugiego. Czas reakcji na uszkodzenia to następny dzień roboczy, w miejscu instalacji rozwiązania.
11. Uszkodzone dyski w czasie gwarancji, które zostaną wymienione na sprawne, muszą pozostać u Zamawiającego.
12. Serwer musi posiadać wolne sloty umożliwiające rozbudowę o dodatkową pamięć operacyjną o minimum 256GB.

13. Serwer musi istnieć możliwość rozbudowy ilości dysków o co najmniej 2 sztuki.
14. Do serwera musi być załączony komplet kabli zasilających oraz prowadnice, uchwyty dla poprawnego montażu w szafie 19 cali.
15. Serwer musi być certyfikowany do pracy z wybranym wirtualizatorem.
16. Dla zapewnienia wysokiej dostępności wymaga się dostawy co najmniej dwóch serwerów tego samego typu i konfiguracji.

Wymagania Licencyjne

1. System SIEM musi współpracować domyślnie (funkcje przygotowane przez producenta rozwiązania przez przedstawieniem oferty) z wszystkimi elementami nowej struktury sieciowej
2. Oferowany SIEM musi zapewnić obsługę w zakresie odbierania logów i monitorowania systemów co najmniej w ilości 80 GB surowych danych na dobę
3. W systemie musi być zapewniona obsługa agentowa co najmniej 92 serwerów.
4. Oferowany SIEM musi być wyposażony w subskrypcje reputacji wskaźników (IOC – indicator of compromise) od tego samego producenta co najmniej w zakresie: adresy IP, domeny, adresy URL. Informacje o reputacji muszą pochodzić z komercyjnego źródła, najlepiej tego samego producenta.
5. Dostarczone licencje muszą być w formie subskrypcji na okres trwania umowy.
6. Dostarczone licencje muszą pozwalać na zbudowanie środowiska bez pojedynczego punktu potencjalnej awarii czyli w pełni redundantnego.

Oferowany system będzie zainstalowany na dedykowanej platformie sprzętowej. Wymaga się, aby na platformie sprzętowej został zainstalowany system wirtualizacyjny, który będzie tworzył klaster maszyn wirtualnych systemu SIEM. System wirtualizacyjny musi być objęty wsparciem technicznym producenta o czasie równym subskrypcji SIEM.

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Komunikacja systemów bezpieczeństwa, z których przesyłane są logi, z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem protokołów/portów: UDP/514.
3. Wydajność SIEM nie może być mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym).
4. SIEM musi być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu

NetFlow.

5. Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:
 - a) aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak: SNMP, Syslog, Windows Management Instrumentation (WMI) i Open Management, Microsoft RPC, Cisco SDEE, Checkpoint LEA, JDBC, VM SDK, Telnet, SSH, HTTPS, IMAP, POP3, import z pliku CSV, REST API
 - b) zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP, TCP, UDP, ICMP, JDBC, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS
6. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
 - a) Ad możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows,
 - b) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application,
 - c) zdolność do monitorowania integralności plików,
 - d) zdolność do monitorowania rejestru systemowego,
 - e) zdolność do monitorowania urządzeń zewnętrznych (removable devices),
 - f) zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów,
 - g) zdolność do wykonywania poleceń WMI wraz z odsyłaniem wyniku ich działania w postaci logów,
 - h) agent instalowany na systemach z rodziny Windows musi komunikować się z SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS,
 - i) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji,
 - j) agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM.
7. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:
 - a) możliwość zbierania logów z wykorzystaniem protokołu syslog,
 - b) możliwość zbierania logów z plików tekstowych,

- c) zdolność do monitorowania integralności plików,
- d) zdolność do monitorowania pliku w oparciu o jego sumę kontrolną,
- e) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu,
- f) zdolność do monitorowania takich parametrów jak obciążenie CPU, zajętość RAM, zajętość dysku, obciążenia sieci, działających aplikacji.

Zbieranie danych:

1. Zebrane dane muszą być przechowywane w sposób skompresowany.
2. SIEM musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji.
3. SIEM nie może wykorzystywać klasycznej relacyjnej bazy danych (np: MS SQL, PostgreSQL, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP.
4. Musi istnieć możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania.
5. Musi istnieć możliwość zbudowania struktury rozproszonej, aby zapewnić większą wydajność zapisu i wyszukiwania.
6. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji.

Korelacja Logów

W zakresie korelacji zdarzeń SIEM 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. SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń. Aktualizacja ta musi być niezależna od oprogramowania systemowego (OS, funkcje wykonawcze, etc.) które ma posiadać swoje wersjonowanie.

4. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System ma korelować zdarzenia co najmniej dla następujących kategorii eventów:
- Malware,
 - Kontroli aplikacji,
 - Email,
 - IPS,
 - Traffic,
 - Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

Raportowanie

W zakresie raportowania SIEM musi zapewniać:

1. SIEM 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 firewalla,
 - g) informacje o realizowanych połączeniach IPSec.
2. Generowanie raportów co najmniej w formatach: CSV, PDF i RTF.
3. Tworzenia raportów z wykorzystaniem graficznego edytora pozwalającego na podgląd pliku PDF przed jego wygenerowaniem.
4. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
5. Funkcję definiowania własnych raportów.
6. Możliwość spolszczenia raportów.
7. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Analityka

System SIEM musi mieć możliwość:

- wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłówów,
- System musi posiadać co najmniej 2000 gotowych reguł korelacyjnych wprowadzonych przez producenta.
- zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN
- wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych,
- wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.
- wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem
- wyszukiwania w oparciu o nie mniej niż następujące operatory: include =, !=, <, >, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex,
- wykorzystania mechanizmów Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym, gdzie system sam decyduje o wyborze optymalnego. W wyniku działania opisanych mechanizmów Machine Learning system ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie.
- wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenia reguł
- tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną
- wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej

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.

2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

X. System ochrony poczty

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów:

- Tryb Gateway,
- Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi dysponować minimum 4 portami Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
3. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
4. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).

5. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
6. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
7. Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
8. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny przez użytkownika.
9. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
10. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
11. Backup poczty realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach przez co najmniej: NFS, iSCSI.
12. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych.
13. Białe i czarne listy adresów oraz domen mailowych dla poszczególnych użytkowników.
14. Zapobieganie przed wyciekami informacji poufnej DLP (Data Leak Prevention).
15. W tym zakresie dostarczony system ochrony poczty musi zapewniać:
 - Skanowanie antywirusowe wiadomości SMTP,
 - Kwarantannę dla zainfekowanych plików,
 - Skanowanie załączników skompresowanych,
 - Definiowanie komunikatów powiadomień w języku polskim,
 - Blokowanie załączników w oparciu o typ pliku,
 - Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antywirusowej.

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. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta,
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania,
3. Szczegółowa kontrola nagłówka wiadomości,
4. Analiza heurystyczna,
5. Współpraca z zewnętrznymi serwerami RBL, SURBL,
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie

- dla całego systemu lub poszczególnych chronionych domen,
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników,
 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF,
 9. Kontrola w oparciu o Greylisting oraz SPF,
 10. Filtrowanie treści wiadomości i załączników,
 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka,
 12. Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antyspamowej,
 13. System musi realizować skanowanie antyspamowe z wydajnością min, 70 tys, wiadomości na godzinę,
 14. Ochrona typu outbrake,
 15. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking),
 16. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości,

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
4. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

Dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG,
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku,
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników,
4. Możliwość podglądu logów w czasie rzeczywistym,
5. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych,
6. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu,
7. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent,
2. Tryb A-P [Active-Passive] z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP,
3. Tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP,
4. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu,
5. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

Dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym,
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów; HTTPS i SSH,
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.

Certyfikaty

System musi posiadać co najmniej certyfikaty: VBSspam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified lub równoważne.

Serwisy i licencje

W ramach Umowy powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Antyspam, URL Filtering, kontrola antywirusowa przez cały okres trwania Etapu II, Sandbox'ing w chmurze przez cały okres trwania Etapu II..

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym przez cały okres trwania Etapu II, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu Wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie

techniczne w dni robocze w godzinach pracy urzędu.

Zaproponowane przez Wykonawcę rozwiązanie w przez cały okres trwania Etapu II musi wykluczyć potrzebę dokupienia jakichkolwiek licencji w przypadku zmiany ilości użytkowników korzystających z poszczególnych systemów. Nie dotyczy to licencji dostępu softwarowego na komputery przenośne, które Wykonawca dostarczy w ilości 3000 szt. oraz nielimitowaną liczbę licencji na smartfony i tablety.

Przez cały okres trwania Etapu II Wykonawca zapewni: aktualizację serwisów i bazy sygnatur, wsparcie techniczne do zastosowanej technologii.

W zakresie zainstalowanych funkcjonalności bezpieczeństwa uruchomionych na urządzeniu ich koszt musi być wliczony w cenę oferty.

Przez cały okres trwania Etapu II Zamawiający ma prawo do skorzystania z nieodpłatnego wykonywania przez Wykonawcę aktualizacji oprogramowania i funkcjonalności na wszystkich zainstalowanych urządzeniach, jeżeli producent tej technologii dostarczy takie aktualizacje. Zasady wykonania usługi Zamawiający i Wykonawca ustalą oddzielnie w trybie roboczym.

XI. System proaktywnej ochrony przed zaawansowanymi zagrożeniami

Zadaniem systemu będzie wykrywanie i blokowanie ataków na infrastrukturę sieci, a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji.

System powinien umożliwiać lokalne logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania. Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API (np. ICAP). Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony Wykonawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania.

System operacyjny

Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.

Parametry fizyczne systemu

System musi posiadać nie mniej niż 2 porty Ethernet 10/100/1000 oraz minimum 2 TB

powierzchni dyskowej. W celu zwiększenia niezawodności system musi mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia. Elementy systemu nie mogą zajmować wysokości większej niż 4U i muszą umożliwiać montaż w standardowej szafie teletechnicznej 19 calowej.

Funkcjonalności podstawowe i uzupełniające

Ochrona przed zaawansowanymi atakami:

- Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z C&C botnetu oraz złośliwymi URL-ami, dostęp do pakietów przeprocesowanych przez dowolny wirtualizator logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.
- Procesowanie plików o rozmiarze co najmniej 8 MB.
- Sandbox dla plików zarchiwizowanych (.tar, .gz, .tgz, .zip, .bz2, .bz, .Z, .cab, .rar, .arj, .7z), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash, JavaArchive (JAR) oraz plików multimedialnych (.avi, .mpeg, .mp3, .mp4),
- Skanowanie protokołów sieciowych: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL, Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszyfrowujących ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowanie ruchu o przepływności 1 Gbps,
- Skanowanie stron WWW z linkami URL,
- Czarne i białe listy dla sum kontrolnych plików,
- Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM,
- Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów PCAP.

Parametry wydajnościowe

Możliwość uruchomienia min. 8 instancji wirtualnych systemów MS Windows w celu wykonania analizy Sandbox w wymiarze co najmniej 150 plików na godzinę.

Zarządzanie

System musi udostępniać:

- Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS,
- Dostęp do CLI przez SSH.

Serwis i usługi

Wykonawca zapewni:

- Gwarancje i serwis przez cały okres trwania Etapu II
- Subskrypcje funkcji bezpieczeństwa przez cały okres trwania Etapu II

Zasilanie

Wszystkie dostarczone elementy systemu powinny być wyposażone w redundantne zasilanie z sieci 230V/50Hz.

XII. Wymagania ogólne Reguły bezpieczeństwa

Wykonawca zaprojektuje przy współpracy z Inspektorem Ochrony Danych Głównego Inspektoratu Pracy oraz Dyrektorem Departamentu Informatyki, a następnie nie później niż w terminie 10 dni roboczych przed rozpoczęciem testów wdroży reguły bezpieczeństwa zapewniające:

- bezpieczny dostęp do Internetu bezpośrednio dla każdej z 62 jednostek organizacyjnych PIP z zastosowaniem urządzeń posiadających funkcjonalności bezpieczeństwa typu: Firewall Stateful Packet Inspection, antywirus, IPS, antyspam, WebFilter, kontrola aplikacji, Data Leak Prevention, i innych wg dostępnych funkcjonalności w ramach dostarczonych technologii,
- kontrolę DLP, tzn. zdefiniuje format niejawnych danych, skonfiguruje blokowanie, logowanie i archiwizowanie wrażliwych danych w systemie PIP WAN oraz zasadę powiadamiania lokalnego administratora i osoby, która nie przestrzega polityki DLP,
- bezpieczne zarządzanie siecią PIP WAN.

Zaproponowane przez Wykonawcę rozwiązanie przez cały okres trwania Etapu II musi wykluczyć potrzebę dokupienia jakichkolwiek licencji w przypadku zmiany ilości użytkowników korzystających z poszczególnych systemów. Nie dotyczy to licencji dostępu softwarowego na komputery przenośne ~~i urządzenia mobilne~~, które Wykonawca dostarczy w ilości 3000 szt.

Przez cały okres trwania Etapu II Wykonawca zapewni aktualne serwisy i sygnatury - jeżeli producent ogłosił aktualizacje. Koszt wszystkich funkcjonalności musi być wliczony w cenę oferty

Przez cały okres trwania Etapu II Zamawiający przewiduje nieodpłatne wykonanie przez Wykonawcę aktualizacji oprogramowania i funkcjonalności na wszystkich zainstalowanych urządzeniach, jeżeli producent dostarczonej technologii w tym okresie udostępni takie aktualizacje.

Wykonawca powiadomi Zamawiającego o ukazaniu się aktualizacji oprogramowania w terminie 14 dni od jej udostępnienia przez producenta. Po przeprowadzeniu testów przez Wykonawcę i potwierdzeniu, że udostępniona aktualizacja oprogramowania nie spowoduje awarii urządzeń i działania sieci oraz po uzyskaniu aprobaty Zamawiającego Wykonawca dokona aktualizacji oprogramowania zgodnie z wcześniej zaakceptowanym przez Zamawiającego harmonogramem.

Aktualizacja oprogramowania nie może nastąpić później niż 7 dni od jej akceptacji przez Zamawiającego.

XIII. Opieka serwisowa

Zamawiający wymaga, aby Wykonawca prowadził 24 godzinny monitoring stanu pracy łącz i urządzeń. W przypadku wykrycia nieprawidłowości, Wykonawca niezwłocznie przystąpi do ich usunięcia i powiadomi o tym fakcie Zamawiającego (e-mail do administratora lokalnego).

Zamawiający wymaga wymiany uszkodzonego urządzenia sieci WAN w godzinach pracy PIP tj. w godz. 8.00 - 16.00 w dni robocze na urządzenie wolne od wad o parametrach nie gorszych niż uszkodzone dla GIP, OIP, OSPIP i OOIP w terminie 9 godzin roboczych od przekazania zgłoszenia przez Zamawiającego.

Zamawiający wymaga usunięcia awarii dla łącza podstawowego w maksymalnie 8 godzin roboczych i łącza zapasowego w maksymalnie 12 godzin roboczych od momentu przekazania zgłoszenia przez Zamawiającego (zgłoszenie do BOK - numer zgłoszenia, e-mail) o wystąpieniu awarii. Zamawiający wymaga potwierdzenia przyjęcia zgłoszenia awarii w formie e-maila nie później niż po upływie 30 minut od momentu przekazania zgłoszenia. Usunięcie awarii łącza ma nastąpić w godzinach pracy Zamawiającego tj. 8.00-16.00 w dni robocze.

Koszt serwisowania i naprawy sprzętu i łącz ponosi Wykonawca.

Koszt dostarczenia i odbioru sprzętu zastępczego do i z poszczególnych jednostek organizacyjnych Państwowej Inspekcji Pracy oraz jego zainstalowania i odinstalowania, a także koszt dojazdu osób, które będą wykonywały ww. czynności pokrywa Wykonawca. Zamawiający wymaga, aby dla dostępowych łącz synchronicznych była zachowana odpowiednia przepustowość określona warstwie 2 modelu ISO OSI, dostępności usługi na poziomie 99 % oraz średnie miesięczne opóźnienia nie większe niż 50 ms.

Wykonawca zobowiązany jest przekazywać Zamawiającemu w okresach kwartalnych informacje o udzielonym wsparciu technicznym, o wszystkich awariach w funkcjonowaniu sieci oraz wykonanych w tym okresie przez Wykonawcę czynnościach w sieci Zamawiającego mailem na adres kancelaria@gip.pip.gov.pl. Informacja musi zawierać: nazwę jednostki zgłaszającej, datę i godzinę

zgłoszenia, czego dotyczyło zgłoszenie, datę i godzinę odpowiedzi, kopię odpowiedzi, datę i godzinę usunięcia awarii. Informacja ma być przekazana w terminie do 10 dni od ostatniego dnia kwartału.

XIV. Administracja systemem

Zamawiający określa następujące zasady administracji systemem PIP WAN:

1. Wykonawca będzie posiadał uprawnienia do zarządzania wszystkimi funkcjonalnościami sieci PIP WAN.
2. Wszyscy administratorzy po stronie Zamawiającego będą się logowali do urządzeń bezpieczeństwa oraz systemu monitoringu parametrów SLA wyłącznie wykorzystując uwierzytelnienia za pomocą minimum loginu i hasła.
3. Po stronie Zamawiającego administratorzy PIP WAN będą posiadali uprawnienia do konfiguracji wszelkich funkcjonalności urządzeń bezpieczeństwa za wyjątkiem następujących:
 - a) konfiguracji bazowej urządzenia tj. routing, adresacji urządzenia, kanałów VPN (jeżeli dotyczy), ustawienia DNS i NTP,
 - b) zarządzania uprawnieniami dostępu w podległych mu urządzeniach,
 - c) usuwania logów z centralnego systemu logowania,
 - d) konfiguracji centralnego systemu zarządzania.
4. Administratorzy Zamawiającego będą posiadali uprawnienia delegowane w dół, tzn.:
 - a) Administratorzy GIP będą posiadali uprawnienia do wszystkich urządzeń bezpieczeństwa dla całej sieci PIP WAN.
 - b) Administratorzy OIP i OSPIP będą posiadali uprawnienia do własnych urządzeń i urządzeń podległych jednostek OOIP oraz wirtualnych systemów zarządzania i monitorowania oraz centralnego logowania odpowiadających własnym jednostkom uruchomionym centralnie w GIP.
 - c) Administrator po stronie Zamawiającego będzie mógł dokonywać wszelkich zmian w ramach podległych obszarowo urządzeń. W szczególności będzie mógł dokonywać zmian polityk bezpieczeństwa, ustaleń QoS, analizy logów (zgodnie z zaleceniami MAiC) itp.
 - d) W przypadku problemów technicznych przy wprowadzaniu zmian we własnym zakresie administrator Zamawiającego będzie mógł zwrócić się o pomoc do Wykonawcy.
 - e) Wykonawca udzieli wsparcia na zgłoszenie Zamawiającego w terminie 2 godzin od przekazania zgłoszenia przez Zamawiającego.
 - f) Logi administracyjne i bezpieczeństwa w systemie PIP WAN zbierane będą lokalnie i centralnie (w szczególności dla każdego węzła: firewall, antywirusa, antymalware, antyspam, IPS, DLP, Web Filtering, kontrola aplikacji). Za przechowywanie logów zgodnie z wymaganiami

określonymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 r. poz.2247 t.j.) odpowiedzialny jest Wykonawca.

g) Zamawiający wymaga, aby odpowiedni administratorzy lokalni Zamawiającego mieli dostęp jedynie do lokalnych logów w trybie do odczytu (np. administrator w OIP Opole jedynie do logów OIP Opole).

5. Dostęp do systemu monitorowania sieci PIP WAN musi być zapewniony administratorom w GIP.
6. Zadaniem Wykonawcy przez cały okres trwania Etapu II jest utrzymywanie w sprawności łącz i urządzeń oraz wsparcie przy rozwiązywaniu problemów konfiguracyjnych.

XV. Adresacja publiczna IP

Wykonawca ma zapewnić w ramach swojego rozwiązania 64 adresy publiczne IP (dodatkowo).

XVI. Testy poprawności konfiguracji urządzeń i sieci PIP WAN

Wykonawca do projektu sieci PIP WAN przedstawi do akceptacji przez Zamawiającego propozycje przeprowadzenia testów w celu potwierdzenia prawidłowego skonfigurowania wszystkich elementów sieci zgodnie z wymaganiami Zamawiającego

XVII. Wymagania dotyczące szkoleń

Wymagania ogólne dotyczące szkoleń

1. Wykonawca przeszkoli pracowników Państwowej Inspekcji Pracy w zakresie budowy i obsługi sieci WAN zbudowanej w Państwowej Inspekcji Pracy.
2. Wykonawca przeszkoli następujące grupy pracowników:
 - 2.1. 18 administratorów PIP (po 1 osobie z każdej jednostki PIP) - szkolenie 2 dniowe.
 - 2.2. 18 zastępców administratorów PIP (po 1 osobie z każdej jednostki PIP) - szkolenie 2 dniowe.
 - 2.3. 6 administratorów centralnych PIP - szkolenie 5 dniowe.
 - 2.4. 18 inspektorów ochrony danych (po 1 osobie z każdej jednostki PIP) - szkolenie 1 dniowe.
3. Szkolenia będą prowadzone w języku polskim.
4. Wykonawca zobowiązany jest przeprowadzić szkolenia po zaakceptowaniu harmonogramu

- dostawy i instalacji urządzeń/oprzysiężowania/oprogramowania oraz uruchomieniu sieci i projektu sieci PIP WAN, ale nie później niż miesiąc przed oddaniem systemu do testów.
5. Szkolenia zorganizowane zostaną na terenie miasta stołecznego Warszawa.
 6. Szkolenia zostaną przeprowadzone w uzgodnionych terminach, w kolejno po sobie następujących dniach od poniedziałku do piątku. Zamawiający nie dopuszcza możliwości realizacji szkoleń dla grup wskazanych w ppkt. 2.1 i 2.2 w tym samym terminie.
 7. W przypadku szkoleń wskazanych w ppkt 2.1, 2.2 i 2.4 Wykonawca zapewni noclegi ze śniadaniami dla uczestników (począwszy od nocy poprzedzającej dzień rozpoczęcia szkolenia) w hotelu o standardzie co najmniej trzygwiazdkowym, usytuowanym w tej samej miejscowości, w której prowadzone będą szkolenia (obiekt zlokalizowany w odległości od miejsca gdzie będą prowadzone szkolenia, umożliwiającej dojazd komunikacją miejską w czasie 45 minut; czas dojazdu liczony będzie razem z dojściem do i od przystanku komunikacji miejskiej). Zamawiający dopuszcza zapewnienie noclegów w motelach, pensjonatach, domach studenckich itp. – pod warunkiem, że będą one spełniały wymagania hotelu trzygwiazdkowego. Budynek oraz pokoje nie mogą posiadać barier architektonicznych dla osób niepełnosprawnych. Zamawiający dopuszcza by nocleg odbywał się w pokojach maksymalnie dwuosobowych – z zastrzeżeniem, że niedopuszczalne jest kwaterowanie osób różnej płci w tych samych pokojach. Zamawiający informuje, że uczestnicy szkolenia z miasta, w którym odbywać się będzie szkolenie, nie będą korzystać z noclegu (natomiast, w przypadku oddelegowania na szkolenie osoby zatrudnionej w oddziale danej jednostki organizacyjnej Państwowej Inspekcji Pracy może wystąpić konieczność zapewnienia dla ww. osoby noclegu).
 8. Zamawiający przekaze Wykonawcy listy uczestników szkoleń wraz z informacją o osobach korzystających z noclegów, w terminie 3 dni od dnia akceptacji dokumentacji, o której mowa w pkt 16. Zamawiający zastrzega, że w przypadku choroby lub wyniknięcia innej szczególnej okoliczności może zmienić uczestnika szkolenia lub zmniejszyć liczbę uczestników danego szkolenia, w tym liczbę osób korzystających z noclegów. O zmianie Zamawiający poinformuje Wykonawcę przed rozpoczęciem danego szkolenia. Zamawiający może zmniejszyć wskazaną w pkt. 2 liczbę uczestników szkoleń (ze wszystkich grup) o maksymalnie 5. Zamawiający informuje, że uiszcza zapłatę tylko za faktyczną liczbę uczestników oraz za faktycznie wykorzystane noclegi oraz kolacje.
 9. Wykonawca zapewni każdemu uczestnikowi szkolenia w każdym dniu szkolenia obsługę: 2 przerw kawowych (gorącą kawę i herbatę, cukier, śmietankę oraz wodę i ciasteczka) i jednej przerwy obiadowej (obiady dwudaniowe).
 10. Wykonawca zapewni uczestnikom szkolenia korzystającym z noclegów, śniadania i kolacje w miejscu zakwaterowania, w każdym dniu szkolenia, z wyjątkiem ostatniego dnia

- szkolenia, w którym nie ma obowiązku zapewnienia kolacji.
11. Zamawiający wymaga, by każde ze szkoleń pierwszego dnia rozpoczynało się najwcześniej o godz. 9.00 i kończyło się najpóźniej o godz. 16.00 dnia ostatniego. Zamawiający wymaga by każdego dnia szkolenia trwały min. 8 godz. (1 godz. = 45 min.). Łączna liczba godzin dla szkolenia pięciodniowego wynosi 40, dla szkolenia dwudniowego – 16, oraz dla szkolenia jednodniowego - 8 godzin.
 12. Wykonawca zapewni niezbędne oprzyrządowanie do przeprowadzenia szkoleń, w tym w szczególności specjalistyczny sprzęt komputerowy odpowiedni do rodzaju zajęć, m.in. indywidualne stanowisko dla każdego uczestnika szkolenia, infrastrukturę sieciową, zainstalowane i skonfigurowane do zajęć odpowiednie oprogramowanie. Szkolenie, o którym mowa w ppkt 2.3. ma mieć charakter warsztatów (każdy z uczestników szkolenia samodzielnie wykonuje ćwiczenia pod nadzorem prowadzącego szkolenie). Sale szkoleniowe muszą być wyposażone w sprzęt prezentacyjny (m.in. projektor, flipchart, tablica). Sale muszą mieć powierzchnię dostosowaną do wielkości grup szkoleniowych. Budynek oraz sala nie mogą posiadać barier architektonicznych dla osób niepełnosprawnych. Wykonawca zapewni materiały piśmiennicze (notatnik, długopis) dla każdego uczestnika szkolenia.
 13. Wykonawca przekaze Zamawiającemu w terminie 7 dni roboczych od dnia rozpoczęcia I Etapu za pośrednictwem poczty elektronicznej, na adres e-mail kancelaria@gip.pip.gov.pl, materiały szkoleniowe (sporządzone w języku polskim). Wykonawca zobowiązany jest do przekazania materiałów szkoleniowych w wersji elektronicznej uczestnikom szkolenia, na co najmniej 3 dni przed terminem szkolenia.
 14. Wykonawca ma obowiązek zapewnić wykładowców posiadających odpowiednie kwalifikacje zawodowe do przeprowadzenia zajęć. Dane ww. osób mają zostać wskazane w Wykazie osób, który będzie stanowił załącznik nr 5 do Umowy.
 15. Wykonawca zobowiązany jest przygotować i wręczyć uczestnikom szkoleń (na zakończenie szkolenia) imienne dokumenty potwierdzające udział w szkoleniu (certyfikaty/dyplomy).
 16. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji w terminie 7 dni roboczych od dnia rozpoczęcia I Etapu na adres wskazany w Umowie, dokumentację szkoleniową zawierającą:
 - a) harmonogram szkoleń, obejmujący terminy i miejsca realizacji szkoleń (co najmniej nazwa i adres budynku) oraz miejsce zakwaterowania (nazwa i adres hotelu).

Zamawiający wymaga, aby szkolenia dla grup wskazanych w ppkt. 2.1 i 2.2 zorganizowane zostały w różnych terminach.

- b) programy szkoleń, które muszą uwzględniać pełny zakres tematyczny szkolenia z podziałem na dni i godziny prowadzenia zajęć i przerw, z podziałem na bloki tematyczne, a w blokach zagadnienia do omówienia, imię i nazwisko wykładowcy; program każdego szkolenia musi uwzględniać, co najmniej tematykę wskazaną w podrozdziale „Minimalny zakres tematyczny szkoleń” (odpowiednią dla każdego rodzaju szkolenia);
 - c) opis metody badania satysfakcji uczestnictwa w szkoleniu oraz projekt karty oceny zawierającej co najmniej punkty dotyczące stopnia omówienia zagadnień ujętych w programie, oceny wiedzy merytorycznej wykładowcy oraz oceny umiejętności dydaktycznych wykładowcy;
 - d) wzór protokołu odbioru szkolenia.
17. Zamawiający uprawniony jest do wniesienia zastrzeżeń do przekazanej dokumentacji szkoleniowej w terminie 3 dni roboczych od jej otrzymania. Uwagi przekazywane będą pocztą elektroniczną (e-mail). Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego i przekazać dokumentację do ponownej akceptacji Zamawiającego w terminie do 2 dni od otrzymania uwag.
18. Wykonawca przekaze Zamawiającemu, wraz z dokumentacją o której mowa w pkt.16, dane co najmniej jednej osoby odpowiedzialnej za realizację szkoleń.
19. Wykonawca przygotuje formularze badania satysfakcji uczestnictwa w szkoleniu i przeprowadzi badania odrębnie dla każdego szkolenia.
20. W terminie 3 dni roboczych od daty zakończenia każdego ze szkoleń, Wykonawca sporządzi (zgodnie z zaakceptowanym wzorem, o którym mowa w pkt 16 ppkt 4) i podpisze protokół odbioru szkolenia w 2 egzemplarzach. Protokoły mają zawierać co najmniej następujące informacje: datę i miejsce przeprowadzenia szkolenia, imię i nazwisko wykładowcy, informację, że uczestnicy szkolenia otrzymali materiały szkoleniowe oraz stwierdzenie, że szkolenie zostało przeprowadzone zgodnie z zakresem obowiązków określonym przez Zamawiającego, miejsce zakwaterowania i liczbę wykorzystanych noclegów. Do protokołów należy załączyć oryginały list uczestników szkolenia (podpisane każdego dnia, przez każdego uczestnika szkolenia), wynik badania satysfakcji wraz z wypełnionymi kartami oceny szkolenia oraz kopie wydanych zaświadczeń/certyfikatów. Protokoły wraz z wymaganymi załącznikami dostarczone do

siedziby PIP GIP będą podpisane przez upoważnionego przedstawiciela Zamawiającego; Osobami uprawnionymi do podpisania protokołów odbioru szkolenia są osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy – zgodnie z zasadami reprezentacji, określonej w KRS, ewidencji działalności gospodarczej lub zgodnie z pełnomocnictwem, zaś po stronie Zamawiającego przez Dyrektora lub Wicedyrektora Departamentu Kadr i Szkoleń PIP GIP.

21. Zamawiający zapłaci Wykonawcy wynagrodzenie za szkolenie dla danej grupy, gdy jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie wyższa niż 3,8 w skali 1-5. W przypadku, gdy ocena merytoryczna szkolenia, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie niższa niż 3,8 pkt w skali 1-5, Strony uznają, że szkolenie dla tej grupy nie zostało wykonane należycie i Wykonawcy nie przysługuje wynagrodzenie. W przypadku nie załączenia przez Wykonawcę do protokołu odbioru szkolenia wyników badania satysfakcji (wraz z wypełnionymi kartami oceny satysfakcji), Zamawiający uzna, że ocena merytoryczna szkolenia na podstawie kart oceny wyników badania satysfakcji była niższa niż 3,8 pkt w skali 1-5 dla danej grupy i Wykonawcy nie przysługuje wynagrodzenie. W przypadkach wskazanych powyżej, Wykonawca zobowiązany będzie przeprowadzić ponownie szkolenie na własny koszt, na warunkach określonych w umowie, w terminie uzgodnionym z Zamawiającym. W takim przypadku koszt wyjazdu służbowego uczestników szkolenia pokrywa Wykonawca (refundacja kosztu zakupu biletów, ryczałtu za dojazdy samochodem prywatnym, diety itp.). Podstawą obliczenia ww. kosztów będą rozliczenia kosztów podróży służbowej (rozliczenia delegacji) uczestników szkolenia przedłożone przez Zamawiającego. W przypadkach wskazanych powyżej, Wykonawcy przysługuje wynagrodzenie po ponownym przeprowadzeniu szkolenia z zastrzeżeniem, że jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie wyższa niż 3,8 w skali 1-5.
22. W przypadku braku możliwości przeprowadzenia szkolenia, w którymkolwiek z terminów, wskazanych w zaakceptowanym przez Zamawiającego harmonogramie szkoleń, Wykonawca zobowiązuje się niezwłocznie poinformować o powyższym Zamawiającego.

W takiej sytuacji Zamawiający ma prawo wskazać termin, w którym ma być przeprowadzone dane szkolenie. Termin wskazany przez Zamawiającego jest wiążący dla Wykonawcy.

23. Zamawiający zastrzega sobie możliwość zmiany terminu szkolenia, w sytuacji losowej związanej z organizacją pracy. Zamawiający niezwłocznie poinformuje o powyższym Wykonawcę oraz przedstawi propozycję nowego terminu szkolenia. Wykonawca będzie zobowiązany, w terminie 3 dni roboczych od dnia otrzymania powyższej informacji, do poinformowania Zamawiającego o możliwości realizacji szkolenia w nowym terminie.
24. Wykonawca uwzględni w ofercie cenowej wszystkie koszty, jakie Państwowa Inspekcja Pracy Główny Inspektorat Pracy będzie zobowiązany ponieść w związku z realizacją szkoleń o których mowa w pkt 2. Zamawiający pokryje jedynie koszt dojazdu uczestników na szkolenie (odrębnie).

Minimalny zakres tematyczny szkoleń

Minimalny zakres tematyczny szkolenia dla administratorów i zastępców

administratorów:

- 1) Wstęp do systemu PIP WAN
 - a) Zasada działania systemu PIP WAN wstęp
 - b) Omówienie funkcjonalności zastosowanych technologii w sieci PIP WAN
 - c) Omówienie sposobu zarządzania systemem PIP WAN: http, console, itp.
 - d) Podstawowa konfiguracja urządzeń
- 2) Koncepcja routingu w sieciach IP
 - a) Routing statyczny
 - b) Routing dynamiczny (OSPF)
 - c) Routing dynamiczny BGP
 - d) BGP: działanie i wybór ścieżki
 - e) Polityki routingu i filtrowanie pakietów
 - f) Obsługa i klasyfikacja ruchu sieciowego: kolejkowanie, szeregowanie, itp.
 - g) Opis zastosowanego routingu w ramach sieci PIP WAN
- 3) Konfiguracja firewalla
 - a) Zasada działania firewalla Stateful Inspection proponowanego urządzenia bezpieczeństwa
 - b) Tworzenie obiektów dla reguł zapory ogniowej
 - c) Reguły uwierzytelniające użytkowników

- d) Traffic shaping, QoS
 - e) Load balancing
 - f) Typowe polityki Firewalla zastosowane w sieci PIP WAN
- 4) Konfiguracja systemu IPS
- a) Zasada działania systemu IPS
 - b) Tworzenie reguł dla systemów IPS w sieci PIP WAN
 - c) Logowanie zdarzeń IPS
 - d) Korelacja zdarzeń
 - e) Typowe polityki IPS uruchamiane w sieci PIP WAN
- 5) SSL-VPN
- a) Koncepcja sieci-VPN
 - b) Architektura SSL-VPN
 - c) Tryby działania SSL-VPN
 - d) Rozwiązania SSL-VPN w sieci PIP WAN
- 6) System zarządzania bezpieczeństwem stacji roboczych oraz konfiguracja klienta VPN
- a) Architektura systemu
 - b) Parametry systemu zarządzania bezpieczeństwem stacji roboczych
 - c) Parametry centralnego systemu zarządzania
 - d) Zdalna konfiguracja klienta VPN stacji roboczej
- 7) Skanowanie antywirusowe
- a) Globalne ustawienia modułu AV
 - b) Filtrowanie plików i obsługa kwarantanny
 - c) Metody i polityki skanowania antywirusowego stosowane w sieci PIP WAN
- 8) Filtracja Antyspamowa
- a) Metody filtrowania spamu
 - b) Obsługa nagłówek MIME
 - c) Konfiguracja czarnych i białych list
 - d) Metody filtrowania spamu oferowanych urządzeń
 - e) Metody i polityki skanowania antyspamowego w sieci PIP WAN
- 9) Filtr stron WWW
- a) Kolejność filtrowania
 - b) Konfiguracja lokalnego filtra stron WWW
 - c) Filtrowanie po zawartości stron

- d) Filtrowanie po kategoriach tematycznych
 - e) Logowanie
 - f) Polityki filtrowania www stosowane w PIP WAN
- 9) Ochrona przed wyciekiem danych - DLP
- a) Metody inspekcji DLP
 - b) Filtrowanie po typie lub po nazwie plików
 - c) Konfiguracja reguł DLP
 - d) Konfiguracja sensora DLP
 - e) Logowanie
 - f) Metody i polityki systemu DLP w sieci PIP WAN
- 10) Kontrola aplikacji
- a) Zasada działania i możliwości
 - b) Konfiguracja listy kontrolowanych aplikacji
 - c) Metody i polityki kontroli aplikacji uruchamiane w sieci PIP WAN
- 11) Optymalizacja ruchu WAN
- a) Dostępne metody optymalizacji
 - b) Konfiguracja i uruchomienie optymalizacji łącz
 - c) Weryfikacja poprawności konfiguracji
 - d) Techniki optymalizacji stosowane w sieci PIP WAN
- 12) Lokalne uwierzytelnianie użytkowników
- a) Metody uwierzytelniania
 - b) Obiekty użytkowników i grup
 - c) Dwuskładnikowe uwierzytelnianie za pomocą tokenów
 - d) Zasada pracy systemu uwierzytelniania w sieci PIP WAN
- 13) Centralne zarządzanie
- a) Opis możliwości systemu zarządzania
 - b) Konfiguracja systemu zarządzania
 - c) Podłączanie urządzeń ochrony w systemie PIP WAN
 - d) Zarządzanie konfiguracją, poszczególnych urządzeń
 - e) Wykorzystanie elementów centralnego zarządzania do zarządzania siecią PIP WAN
- 14) Logowanie i monitoring
- a) Konfiguracja logowania dla zdarzeń systemowych
 - b) Konfiguracja protokołu Syslog i SNMP

- c) Rejestracja i konfiguracja centralnego systemu logowania
 - d) Korelacja zdarzeń na podstawie logów
 - e) Analiza logów systemowych i logów bezpieczeństwa
 - f) Konfiguracja alertów mailowych
- 15) Zakres podstawowych czynności administracyjnych w ramach PIP WAN
- 16) Troubleshooting - procedury awaryjne i naprawcze
- 17) Konfigurowanie Access Pointa

Minimalny zakres tematyczny szkolenia dla administratorów centralnych:

Szkolenie ma obejmować obsługę i administrację systemów centralnie zarządzanych: analizę logów i raportowania, system analizy i korelacji zdarzeń w sieci, centralne zarządzanie siecią, ochronę przed atakami DDOS, systemu monitoringu parametrów SLA dla sieci PIP WAN oraz zakres zaawansowanych czynności administracyjnych w ramach PIP WAN, w tym:

- 1) Analiza logów i raportowanie
 - a) Cele zbierania logów
 - b) Budowa logów bezpieczeństwa
 - c) Budowa logów systemowych
 - d) Synchronizacja czasu w systemie logowania
 - e) Najlepsze praktyki i konfiguracje systemów logujących zdarzenia bezpieczeństwa i systemowych
 - f) Zabezpieczenie logów
- 2) System korelacji logów zdarzeń w sieci
 - a) Umieszczenie centralnego i lokalnego systemu logowania
 - b) Analiza logów pod względem występowania anomalii
 - c) Automatyczna i ręczna analiza logów
 - d) Praktyczne przykłady korelacji logów systemowych i bezpieczeństwa
 - e) Konfigurowanie mechanizmów powiadomień administratorów w sytuacjach szczególnych
- 3) Centralne zarządzanie siecią
 - a) Zaawansowane funkcje administracyjne
 - b) Określenie poziomu uprawnień
 - c) Tworzenie polityk i reguł stosowanych w urządzeniach pracujących w sieci PIP WAN
 - d) Wykorzystanie centralnego systemu zarządzania siecią w sytuacjach szczególnych

- 4) Konfiguracja systemu zapewniającego ochronę przed atakami DDOS
 - a) Architektura i zasada działania systemu anty-DDOS
 - b) Typy ataków DDOS
 - c) Konfiguracja ochrony usługi WWW, DNS
- 5) Wysoka dostępność
 - a) Zasada i tryby działania
 - b) Konfiguracja klastrów HA systemu PIP WAN
 - c) Zasada działania klastrów wysokiej dostępności w stosowanych w sieci PIP WAN
- 6) System monitoringu parametrów SLA w sieci PIP WAN
 - a) Zasada działania systemu monitorowania parametrów SLA sieci PIP WAN
 - b) Rodzaje i charakterystyka używanych protokołów
 - c) Budowa dostarczonego w ramach umowy systemu monitorowania parametrów SLA sieci PIP WAN
 - d) Konfiguracja narzędzia: instalacja, przegląd domyślnych ustawień, widoki, aktualizacja, archiwizacja
 - e) Rozwiązywanie problemów z siecią. Zastosowanie raportów do analizy sieci. Główne zakładki. Analiza historycznych danych. Tworzenie raportów
 - f) Śledzenie parametrów SLA sieci PIP WAN. Kontrola pasma. Kontrola QoS. Pomiar gwarantowanej przepustowości
 - g) Monitorowanie proaktywne. Przedstawienie możliwości tworzenia harmonogramów raportów oraz profili powiadomień

Minimalny zakres tematyczny szkolenia dla inspektorów ochrony danych:

Uwaga: większość uczestników tego szkolenia nie ma wykształcenia technicznego, w związku z tym szkolenie musi być dostosowane do wiedzy i umiejętności w tym zakresie grupy szkoleniowej. Zakres tematyczny jest następujący:

- 1) Podstawy zabezpieczania sieci - systemy Firewall
 - a) typy Firewalli
 - b) konfiguracja Firewalla
 - c) ustalanie zestawu reguł Firewalla
 - d) systemy UTM
- 2) Ataki na systemy - DoS, IP spoofing, DNS spoofing, spamming, crack, SYN flooding, buffer overflow, konie trojańskie, ataki z wykorzystaniem WWW

3) Systemy wykrywania włamań

- a) IDS hostowy
- b) IDS sieciowy
- c) określanie zasad monitorowania zdarzeń
- d) reakcje na incydent

4) HoneyPot - „garnek miodu”

- a) typy honeypotów
- b) instalacja i konfiguracja

5) Kontrola ruchu sieciowego

- a) analiza ruchu sieciowego
- b) natężenie ruchu i statystyki
- c) SNMP w analizie ruchu sieciowego
- d) RMON
- e) Netflow
- f) Sflow

6) Zarządzanie logami

- a) logi systemowe
- b) logi z systemów bezpieczeństwa
- c) strategia archiwizacji logów