

## Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa wraz z usługą wdrożenia systemu bezpieczeństwa brzegu sieci dla jednostek PGL Lasy Państwowe w postaci nieużywanych, fabrycznie nowych urządzeń typu Firewall UTM wraz z systemem centralnego zarządzania oraz logowania, systemem gwarancji, licencji oprogramowania oraz wsparcia technicznego.

W ramach uruchomienia konieczne jest wykonanie następujących czynności:

- a) Szkolenie certyfikowane z obsługi i zarządzania urządzeniami klasy UTM producenta urządzeń dla Administratorów Centralnych;
- b) Konsultacje między Zamawiającym a Wykonawcą w celu opracowania strategii wdrożenia;
- c) Przygotowanie oraz dostawa nowych urządzeń Firewall UTM do wskazanych oddziałów przez Zamawiającego;
- d) Przygotowanie i przeniesienie konfiguracji w zakresie zdefiniowanym przez Zamawiającego;
- e) Uruchomienie nowych urządzeń Firewall UTM z ustaloną konfiguracją w infrastrukturze Zamawiającego;
- f) Szkolenie powdrożeniowe dla Administratorów Regionalnych;
- g) Serwisu infrastruktury wdrożonego rozwiązania w zakresie zdefiniowanym przez Zamawiającego;

### 1. Wymagania ogólne

- 1) Wszystkie urządzenia muszą pochodzić z oferty jednego producenta;
- 2) Wszystkie wyspecyfikowane wartości muszą zostać potwierdzone w oficjalnej dokumentacji producenta oferowanego rozwiązania.
- 3) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- 4) Dostarczony system bezpieczeństwa musi zapewniać wymienione funkcje sieciowe jak i bezpieczeństwa niezależnie od dostawcy łącza;
- 5) Wszystkie urządzenia muszą być fabrycznie nowe, nieużywane wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia, oznaczone symbolem CE tam gdzie jest to wymagane, pochodzić z legalnego źródła oraz być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Oferowane modele muszą znajdować się w sprzedaży, co najmniej od 30 dni poprzedzających termin złożenia oferty;
- 6) Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje, które mogą zostać złożone w oryginale lub kopii poświadczającej zgodność z oryginałem:
  - a) ICSA Labs lub EAL4 dla funkcji Firewall lub Common Criteria Protection Profiles lub NSS Labs;
- 7) Urządzenia muszą być urządzeniami o uznanej na rynku pozycji i muszą znajdować się w kwadracie „Leaders” raportu Gartnera pt. „Magic Quadrant of Network Firewalls” na rok 2020 oraz 2021;
- 8) Wykonawca składając ofertę potwierdza, że dostarczone urządzenia spełniają wszystkie wymagania zawarte w OPZ. Wykonawca przedstawi kartę produktu

zawierającą opis funkcjonalności i parametry, zamawiający dopuszcza wersję angielską.

- 9) Dopuszcza się, by system centralnego zarządzania i logowania (Grupa IV), wchodzący w skład systemu ochrony był zrealizowany w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej dedykowanej platformy „virtual appliance”.
- 10) System musi działać jako jedna całość i być uruchomiony w Centrum Podstawowym (CP) przetwarzania danych Zamawiającego oraz wyznaczonych jednostkach PGL Lasy Państwowe;

System bezpieczeństwa firewall UTM zapewnia pełne zarządzanie dostępem do brzegu sieci zasobów jednostek, realizując przy tym takie same wsparcie dla usług jak w przypadku routera (L3) wzbogaconego o szereg zabezpieczeń i funkcji chroniących przed potencjalnymi atakami z zewnątrz jak i wewnątrz sieci. Obejmuje kontrolą ochronę antywirusową, treści WWW, zaporę sieciową, system prewencji włamań (IPS), system detekcji zagrożeń (IDS), kontrolę aplikacji i usług.

Cały system podzielony został na cztery grupy:

- Grupa I – urządzenia instalowane w Nadleśnictwach, Zakładach i Ośrodkach LP,
- Grupa II – urządzenia instalowane w Regionalnych Dyrekcjach LP i Zakładach LP,
- Grupa III – urządzenia instalowane w Dyrekcji Generalnej LP,
- Grupa IV – system centralnego zarządzania i logowania instalowany w CP.

## **2. Wymagania dla I Grupy urządzeń typu Firewall UTM dla Nadleśnictw, Zakładów i Ośrodków.**

- 1) System realizujący funkcję Firewall musi dysponować:
  - a) minimum 6 portami GigabitEthernet RJ-45;
- 2) W ramach systemu Firewall powinna być możliwość zdefiniowania na jednym porcie urządzenia VLAN'y w oparciu o standard 802.1Q w ilości co najmniej: 30 interfejsów wirtualnych
- 3) W zakresie Firewall'a obsługa:
  - a) minimum 37 tys. nowych sesji na sekundę TCP;
- 4) Przepustowość ruchu Firewall z włączoną funkcją kontroli aplikacji (pakiet 64KB HTTP): minimum 1,8 Gbps;
- 5) Wydajność dla ruchu IPSec VPN (AES-256): nie mniej niż 1,2 Gbps;
- 6) Przepustowość ruchu dla kontroli NGFW (Firewall, Application Control, IPS, antymalware) dla ruchu typu Enterprise\*: minimum 0,9 Gbps;
- 7) Architektura urządzeń powinna być wyposażona w osobne układy odpowiedzialne za przetwarzanie funkcji sieciowych/bezpieczeństwa i funkcje ogólnego przeznaczenia;
- 8) Urządzenie musi być wyposażone w uchwyty/szyny do montażu urządzeń w szafie RACK 19”.
- 9) Maksymalna wysokość urządzenia w szafie RACK 1U.

\*ruch Enterprise (HTTPS - 32%; HTTP – 5%; LDAP – 25%; DNS – 1,6%; SMTP – 3,9%; UDP – 2,5%; TCP – 30%)

**3. Wymagania dla II Grupy urządzeń typu Firewall UTM dla jednostek Regionalnej Dyrekcji Lasów Państwowych i Zakładów.**

- 1) System realizujący funkcję Firewall musi dysponować:
  - a) minimum 6 portami GigabitEthernet RJ-45;
- 2) W ramach systemu Firewall powinna być możliwość zdefiniowania na jednym porcie urządzenia VLAN'y w oparciu o standard 802.1Q w ilości co najmniej: 30 interfejsów wirtualnych;
- 3) Musi dysponować minimum dwoma redundantnymi zasilaczami AC;
- 4) W zakresie Firewall'a obsługa: minimum 55 tys. nowych sesji na sekundę TCP;
- 5) Przepustowość ruchu Firewall z włączoną funkcją kontroli aplikacji (pakiet 64KB HTTP): minimum 2,2 Gbps;
- 6) Wydajność dla ruchu IPSec VPN (AES-256): nie mniej niż 3 Gbps;
- 7) Przepustowość ruchu dla kontroli NGFW (Firewall, Application Control, IPS, antymalware) dla ruchu typu Enterprise\*: minimum 1,2 Gbps;
- 8) Architektura urządzeń powinna być wyposażona w osobne układy odpowiedzialne za przetwarzanie funkcji sieciowych/bezpieczeństwa i funkcje ogólnego przeznaczenia;
- 9) Urządzenie musi być wyposażone w uchwyty/szyny do montażu urządzeń w szafie RACK 19'.
- 10) Maksymalna wysokość urządzenia w szafie RACK 2U.

\*ruch Enterprise (HTTPS - 32%; HTTP – 5%; LDAP – 25%; DNS – 1,6%; SMTP – 3,9%; UDP – 2,5%; TCP – 30%)

**4. Wymagania dla III Grupy urządzeń typu Firewall UTM dla jednostki Dyrekcji Generalnej Lasów Państwowych.**

- 1) System realizujący funkcję Firewall musi dysponować:
  - a) minimum 6 portami GigabitEthernet RJ-45;
  - b) minimum 4 porty GigabitEthernet SFP;
  - c) minimum 2 porty 10 GigabitEthernet SFP+;
- 2) W ramach systemu Firewall powinna być możliwość zdefiniowania na jednym porcie urządzenia VLAN'y w oparciu o standard 802.1Q w ilości co najmniej: 30 interfejsów wirtualnych;
- 3) Musi dysponować minimum dwoma redundantnymi zasilaczami AC;
- 4) W zakresie Firewall'a obsługa: minimum 160 tys. nowych sesji na sekundę TCP;
- 5) Przepustowość ruchu Firewall z włączoną funkcją kontroli aplikacji (pakiet 64KB HTTP): minimum 13Gbps;
- 6) Wydajność dla ruchu IPSec VPN (AES-256): nie mniej niż 4,5 Gbps;
- 7) Przepustowość ruchu dla kontroli NGFW (Firewall, Application Control, IPS, antymalware) dla ruchu typu Enterprise\*: minimum 2,5 Gbps;
- 8) Możliwość pracy w trybie HA: co najmniej Active/Active, Active/Passive
- 9) Architektura urządzeń powinna być wyposażona w osobne układy odpowiedzialne za przetwarzanie funkcji sieciowych/bezpieczeństwa i funkcje ogólnego przeznaczenia;
- 10) Urządzenie musi być wyposażone w uchwyty/szyny do montażu urządzeń w szafie RACK 19'.
- 11) Maksymalna wysokość urządzenia w szafie RACK 3U.
- 12) Wkładki w ilości min. dwóch kompatybilnych z oferowanym urządzeniem oraz min. dwóch kompatybilnych z urządzeniami pracującymi w infrastrukturze zamawiającego

dla urządzeń „CISCO” wkładki SFP+ winny być określone parametrami multi-mode; min. 10,0Gbps (SFP+); 2xLC (duplex); długość fali (TX/RX): 850nm; odległość transmisji do 300m; Układ Diagnostyki / Monitoring; Hot-Pluggable wraz z patchcordami światłowodowymi w ilości min. dwóch o długości min. 15m;

\*ruch Enterprise (HTTPS - 32%; HTTP – 5%; LDAP – 25%; DNS – 1,6%; SMTP – 3,9%; UDP – 2,5%; TCP – 30%)

#### **5. Wymagania dla IV Grupy urządzeń centralnych do zarządzania i logowania w CP.**

- 1) W ramach postępowania musi zostać dostarczony niezależny od działających systemów w infrastrukturze Zamawiającego, autonomiczny system centralnego zarządzania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. System centralnego zarządzania i logowania musi pochodzić od producenta oferowanych urządzeń bezpieczeństwa oraz umożliwiać zarządzanie wszystkimi wymaganymi w ramach postępowania systemami pełniącymi funkcję firewall UTM. W przypadku realizacji programowej system może zostać zainstalowany na platformie wirtualizacji Zamawiającego;
- 2) Zamawiający informuje, iż posiada dostępne zasoby sprzętowe dla systemu działającego w środowisku Vmware dla ESXi 6.x i nowszych w określonych ilościach: 32 vCPU, 64 GB RAM, przestrzeń dyskowa 15TB NVMe oraz 30TB SAS R6 dla całego systemu zarządzającego-raportującego. Jeżeli zasoby sprzętowe przeznaczone przez Zamawiającego na system do zarządzania i logowania nie spełnia wymagań producenta co do prawidłowej i stabilnej obsługi wszystkich urządzeń z grupy I-III, wtedy Wykonawca musi dostarczyć sprzęt (serwer/serwery), platformę wirtualizacyjną, system dyskowy oraz niezbędne licencje. Dostarczona platforma sprzętowo-wirtualizacyjna musi zostać podłączona do posiadanego przez Zamawiającego Vmware vCenter w wersji 6.7 lub nowszej. W przypadku instalacji oprogramowania na sprzęcie i platformie wirtualizacyjnej Zamawiającego, Wykonawca musi wziąć pod uwagę warunki dostarczanych licencji i dostarczyć licencję dla wdrażanego systemu w środowisku Zamawiającego składającego się z platformy wirtualizacyjnej Vmware. Zasoby serwerowe przeznaczone do wdrożenia znajdują się w klastrze DataCenter składającym się z 10 serwerów ESXi po dwa CPU każdy, suma 20 CPU (20 socket)
- 3) Wykonawca dostarczy niezbędne licencje, konieczne do uruchomienia platformy programowej systemu w środowisku Vmware
- 4) System centralnego zarządzania musi zapewnić scentralizowane, oparte na automatyzacji zarządzanie wszystkimi urządzeniami z jednej konsoli dla pełnej administracji i widoczności elementów sieciowych;
- 5) System centralnego zarządzania powinien posiadać możliwość użycia szablonów do aktualizacji oprogramowania sprzętowego oraz zdalnego wdrażania nowych urządzeń.
- 6) System centralnego logowania musi zapewnić zarządzanie logami, analizę i raportowanie danych z urządzeń firewall UTM.
- 7) System zarządzania powinien posiadać możliwość weryfikacji wszystkich licencji dostępnych oraz zainicjowanych na urządzeniach Firewall UTM;
- 8) W ramach centralnego systemu zarządzania urządzeniami firewall UTM rozwiązanie musi posiadać właściwe licencje, jeżeli są wymagane oraz zapewnić obsługę:
  - a) minimum 500 urządzeń firewall UTM;

- 9) W ramach centralnego systemu logowania zdarzeń występujących na urządzeniach firewall UTM rozwiązanie musi posiadać właściwe licencje, jeżeli są wymagane oraz zapewnić obsługę:
  - a) minimum 500GB danych logów zdarzeń dziennie;
  - b) obsługę nie mniej niż 45TB przestrzeni dyskowej;
- 10) System musi umożliwiać uwierzytelnienie i autoryzację użytkowników administracyjnych zarządzających systemem centralnego zarządzania i logowania zdarzeń w ramach sesji, gdzie dostawcą tożsamości będą:
  - a) Wewnętrzna baza danych użytkowników;
  - b) Zewnętrzne bazy LDAP (w tym Active Directory);
  - c) Serwery RADIUS;
- 11) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
- 12) Dostarczone rozwiązanie musi posiadać możliwość definicji uprawnień dla różnych grup Administratorów do poszczególnych części „drzewa” konfiguracji.
- 13) Musi być zapewniona możliwość jednoczesnego wysyłania logów do co najmniej dwóch serwerów logowania zdarzeń działających jako klaster.
- 14) System musi mieć możliwość zarządzania przez systemy firm trzecich wykorzystując API, do którego producent udostępni dokumentację.
- 15) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

#### **6. Wymagania wspólne dla I,II,III Grupy urządzeń tworzących system bezpieczeństwa.**

##### **Wspólne dla wszystkich grup urządzeń.**

- 1) Urządzenia oferowane przez Wykonawcę muszą wspierać architekturę SD-WAN;
- 2) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS, SSH oraz port konsoli szeregowej, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania;
- 3) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma oraz wskazanie priorytetu ruchu;
- 4) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji;
- 5) System musi umożliwić korzystanie z predefiniowanej bazy adresów URL pogrupowanych w kategorie tematyczne, z możliwością definiowania własnych list wyjątków oraz własnych sygnatur URL;
- 6) Współpraca z krajową siecią energetyczną o parametrach : 230/240V AC, 50/60 Hz;
- 7) W zakresie routingu rozwiązanie powinno zapewniać obsługę:
  - a) Routingu statycznego;
  - b) Policy Based Routingu;
  - c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP;
- 8) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP.
- 9) System Firewall musi posiadać gniazdo USB umożliwiające inicjalizację pliku konfiguracyjnego;
- 10) System musi wspierać IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w Warstwie Aplikacji, Protokołów routingu dynamicznego;
- 11) Urządzenia muszą posiadać funkcjonalność DHCP;
- 12) Urządzenia muszą umożliwiać możliwość pracy w jednym z trzech trybów: Router/NAT, Transparent lub Monitorowania na porcie SPAN;

- 13) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów;
- 14) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- 15) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- 16) W ramach logowania system pełniący funkcję Firewall UTM musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.
- 17) Musi istnieć możliwość logowania do serwera SYSLOG.
- 18) Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne.
- 19) W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, Dynamic DNS, proxy.
- 20) Filtr WWW musi dostarczać kategorii stron zabronionych prawem.
- 21) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur, białe/czarne listy dla adresów URL.
- 22) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- 23) W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
- 24) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- 25) Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 26) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- 27) Baza aplikacji powinna zawierać kategorie, szczególnie istotne z punktu widzenia bezpieczeństwa, które muszą uwzględniać co najmniej aplikację typu: P2P, Proxy, VPN, Tor, Remote Access. System musi posiadać możliwość tworzenia własnych sygnatur dla aplikacji własnych.
- 28) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- 29) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- 30) Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- 31) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- 32) Mechanizmy ochrony dla aplikacji Web'owych co najmniej ochrona przed: Cross-site Scripting, SQL Injecton, Brute force.
- 33) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- 34) Dostarczony system musi posiadać możliwość definiowania własnych list wskaźników IoC tj. sieci i adresy IP, nazwy DNS, skróty plików (co najmniej: SHA, MD5). Jeżeli jest

to wymagane Wykonawca musi dostarczyć odpowiednie licencje producenta w ramach wskazanego rozwiązania;

- 35) System musi umożliwiać kontrolę zawartości plików PDF oraz MS Office w przypadku wykrycia zagrożenia musi posiadać możliwość zablokowania oraz raportowania zagrożenia.
- 36) System musi posiadać możliwość współpracy z usługą typu Sandbox w wersji chmurowej, z możliwością zarządzania i definiowania jakie dane będą przekazywane do zewnętrznych usług producenta. Jeżeli jest to wymagane Wykonawca musi dostarczyć odpowiednie licencje producenta w ramach wskazanego rozwiązania;
- 37) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- 38) System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR.
- 39) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
- 40) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji (L7) oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
- 41) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- 42) Monitoring stanu realizowanych połączeń VPN.
- 43) Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
- 44) Kontrola Aplikacji (L7).
- 45) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- 46) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
- 47) Ochrona przed atakami - Intrusion Prevention System.
- 48) Kontrola stron WWW.
- ~~49) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.~~
- 50) Zarządzanie pasmem (QoS, Traffic shaping) za pomocą polityk powinny umożliwiać określenie adresów IP, portów, protokołów, aplikacji, użytkownika lub grupy użytkowników w oparciu o zewnętrznych dostawców tj. AD, zawierać pola DSCP.
- 51) Obsługa tuneli GRE.
- 52) Analiza ruchu szyfrowanego protokołem SSL.
- 53) System powinien zapewnić możliwość tworzenia polityk bezpieczeństwa z uwzględnieniem:
  - a) Adresów i sieci IPv4/IPv6;
  - b) Użytkowników;
    - Użytkowników oraz grupy przechowywane w lokalnej bazie systemu,
    - Użytkowników, grupy zagnieżdżone przechowywane w bazach zgodnych z LDAP,
    - ~~- Atrybutów VSA zwracanych po uwierzytelnieniu użytkownika w serwerze RADIUS.~~
    - ~~- Użytkowników oraz grupy przechowywane w bazach zgodnych z TACACS+;~~
  - c) Protokołów i portów sieciowych;
  - d) Usług sieciowych;
  - e) Aplikacji i ich zbiorów;
  - f) List reputacji;

- g) Wskaźników IoC;
  - h) Uruchomienie poszczególnych modułów funkcjonalnych zabezpieczeń tj. IPS, AV itd..., indywidualnie dla każdej stworzonej polityki bezpieczeństwa,
  - i) Logowanie zdarzeń w odniesieniu do poszczególnych polityk bezpieczeństwa;
- 54) System musi mieć możliwość tworzenia dynamicznych obiektów adresowych do których, na podstawie zdefiniowanych etykiet, można w automatyczny sposób przypisywać adresy IP. Powinna istnieć możliwość ręcznego tworzenia etykiet bezpośrednio w systemie zarządzania lub automatycznego pobierania ich z zewnętrznych systemów np. Vmware vCenter oraz skojarzonych z tymi etykietami adresów IP. Powinna istnieć możliwość wykorzystania tak zbudowanych obiektów adresowych w politykach bezpieczeństwa.
- 55) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
- a) Translację jeden do jeden oraz jeden do wielu.
  - b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- 56) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- 57) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:
- a) Amazon Web Services (AWS);
  - b) Microsoft Azure;
  - c) Cisco ACI;
  - d) Google Cloud Platform (GCP)
  - e) OpenStack;
  - f) Vmware vCenter (ESXi);
- 58) System musi umożliwiać konfigurację połączeń typu IPSec VPN. Zakres tej funkcji musi zapewniać:
- a) Wsparcie dla IKE v1 oraz v2.
  - b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
  - c) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh;
  - d) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
  - e) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
  - f) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
  - g) Obsługa mechanizmów: IPSec NAT Traversal, DPD.
  - h) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
- 59) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
- a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
  - b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
  - c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

## 7. Specyfikacja zestawienia ilościowego dla poszczególnych grup sprzętowych:

Lp.	Grupy sprzętowe wg. wymagań:	Przeznaczenie:	Liczba urządzeń:
1.	I Grupa urządzeń	Firewall UTM dla Nadleśnictw, Zakładów i Ośrodków	452 szt.
2.	II Grupa urządzeń	Firewall UTM dla jednostek Regionalnej Dyrekcji Lasów Państwowych i Zakładów	19 szt.
3.	III Grupa urządzeń	Firewall UTM dla jednostki Dyrekcji Generalnej Lasów Państwowych	2 szt.
4.	IV Grupa urządzeń	System centralnego zarządzania i logowania instalowany w CP	1 szt.

## 8. Szczegółowy zakres wdrożenia:

W ramach wykonania usługi wdrożeniowej Wykonawca zobowiązany jest do:

- 1) Wykonania audytu obecnej topologii sieci oraz użytych mechanizmów sieciowych pod kątem wybrania najbardziej optymalnej topologii docelowej.
- 2) Wykonania audytu konfiguracji i działania obecnie posiadanych urządzeń sieciowych, którego konfiguracja ma stanowić punkt wyjścia do opracowania koncepcji wdrożenia nowego systemu firewall. W zakresie filtracji ruchu należy założyć, że obecna polityka bezpieczeństwa jest uboga i winna być zbudowana praktycznie od nowa.
- 3) Analiza użycia używanych obecnie połączeń oraz przepływu danych w sieci pod kątem aktywnego wykorzystania przez poszczególne usługi i aplikację,
- 4) Analiza wymogów bezpieczeństwa u Zamawiającego pod kątem przyszłej polityki na firewallu włącznie z wywiadem środowiskowym w celu uzupełnienia wiedzy i analizą działania poszczególnych aplikacji w celu określenia używanych portów TCP/UDP.
- 5) Przygotowania koncepcji zmian w topologii, jeśli takie będą wymagane, do osiągnięcia najbardziej optymalnej pod względem szybkości działania i niezawodności topologii docelowej.
- 6) Przygotowanie koncepcji wdrożenia nowych urządzeń UTM uwzględniając aspekt współpracy/integracji z sąsiednimi systemami i urządzeniami (typu przełączniki rdzeniowe, Active Directory), oraz przedstawione przez administratorów wymagania.
- 7) Koncepcja wdrożenia poza tradycyjnymi elementami typu reguły filtracji oraz translacji powinna obejmować szczegółowe wdrożenie wszystkich obsługiwanych przez firewall funkcji UTM, tunele VPN (typu IPSec oraz SSL), jak również identyfikację użytkowników z wykorzystaniem kont w Active Directory
- 8) Przygotowanie awaryjnej procedury "rollback" na wypadek niepowodzenia wdrożenia, gwarantującego szybki powrót do stanu pierwotnego zapewniając podtrzymanie poprawnej pracy usług biznesowych.
- 9) Wdrożenia systemu do centralnego zarządzania wszystkimi dostarczonymi urządzeniami UTM. W systemie centralnego zarządzania powinny zostać zdefiniowane grupy urządzeń i szablony polityk bezpieczeństwa uwzględniające powyższe aspekty
- 10) Wdrożenie systemu do gromadzenia logów wraz z integracją ze wszystkimi urządzeniami UTM
- 11) Stworzenie centralnej bazy obiektów i polityk dla wszystkich urządzeń UTM

- 12) Wdrożenie firewalli UTM w 11 jednostkach pilotażowych w sieci WAN PGL LP wyszczególnionych w Załącznik nr 10 do Umowy. Należy w szczególności wykonać:
  - a. Konfigurację routingu statycznych na firewallu a w razie potrzeby wdrożenia routingu dynamicznego (RIP, OSPF, BGP),
  - b. Konfigurację polityki bezpieczeństwa zgodnie z wytycznymi ze strony Zamawiającego, nie naruszając wymogów bezpieczeństwa u Zamawiającego.
  - c. Konfigurację filtracji stron WWW na podstawie kategorii oraz treści,
  - d. Integrację firewalla z systemem autoryzacji Microsoft Active Directory w trybie transparentnym lub przy użyciu dedykowanych agentów (system musi umożliwiać obydwa tryby integracji a Zamawiający podczas wdrożenia wybierze właściwy), tak aby możliwa była identyfikacja użytkowników
- 13) Wdrożenie firewalli UTM na styku dedykowanej sieci WAN PGL LP z uwzględnieniem wszystkich przedstawionych wymagań i zaakceptowanej przez Zamawiającego koncepcji. Prace należy w szczególności wykonać zgodnie z ww. punktem a-d.
- 14) Wykonania rekonfiguracji innych urządzeń i systemów w sieci w celu poprawnej współpracy z firewallami (uruchomienie agregacji portów LACP, rekonfiguracja STP, integracja z AD itp).
- 15) Przygotowanie koncepcji wdrożenia łącz zapasowych z wykorzystaniem SD-WAN.
- 16) Wykonania testów niezawodności i odporności na różne awarie i scenariusze zdarzeń (awaria linku, urządzenia, zapętlenie ruchu w switchu w dowolnej strefie, awaria dowolnego portu w firewallu).

**9. Warunki licencjonowania oraz system gwarancyjny:**

- 1) Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancji i procedury awarii, dostępne kanały komunikacyjne z serwisem producenta i wykonawcy.
- 2) Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:
  - a) Wsparcie wykonawcy oraz serwis urządzeń wdrożonego systemu zgodnie z okresem obowiązywania Umowy, przy czym okres wsparcia oraz serwisu urządzeń liczony jest od dnia podpisania protokołu odbioru końcowego przedmiotu zamówienia,
  - b) Wykonawca w ramach wsparcia zapewni Zamawiającemu 24 godziny konsultacji w skali miesiąca przez cały okres obowiązywania Umowy.
  - c) Przyjmowanie w ramach serwisu zgłoszeń Zamawiającego przez 24 godziny na dobę, 7 dni w tygodniu.
  - d) Czas reakcji serwisu to maksymalnie cztery godziny od momentu przyjęcia zgłoszenia. Przyjęcie zgłoszenia powinno następować automatycznie po jego dokonaniu i zostać potwierdzone przez Wykonawcę wiadomością elektroniczną na wskazany adres e-mail ..... Czas reakcji rozumiany jest jako podjęcie działań diagnostycznych, czynności zmierzających do naprawy.
  - e) Czas naprawy nie może przekroczyć dwudziestu czterech godzin liczonych od chwili przyjęcia zgłoszenia. Czas naprawy rozumiany jest jako czas usunięcia przez Wykonawcę zgłoszonego przez Zamawiającego problemu.
  - f) Zamawiający dopuszcza, w przypadku wystąpienia problemu krytycznego, zastosowanie procedury awaryjnej, która zakłada doraźne wykorzystanie rozwiązania tymczasowego, rozwiązującego problem krytyczny.
  - g) Wymianę urządzeń w przypadku zdiagnozowania awarii powodującej całkowity brak możliwości korzystania z Urządzenia.

- h) Możliwość naprawy lub wymiany urządzeń w przypadku jego wadliwości, tym samym w przypadku naprawy wadliwego urządzenia Wykonawca zobowiązany będzie udostępnić na czas naprawy identyczne urządzenie zastępcze Zamawiającemu.
- i) *Gwarancję producenta wraz z licencjami obejmującą wszystkie dostarczone Urządzenia wraz z oprogramowaniem, przy czym bieg okresu gwarancji oraz licencji w tym subskrypcji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu końcowego odbioru przedmiotu Umowy.*
- j) W ramach postępowania Wykonawca dostarczy licencje równoważne z subskrypcją upoważniające do korzystania z aktualnych baz funkcji ochrony producenta obejmujące: kontrolę aplikacji, IPS, Antywirus, Web Filtering baz reputacji adresów IP/domen.
- k) Możliwość aktualizacji oprogramowania przez dostęp do zasobów producenta.
- l) Możliwość zgłoszenia awarii bezpośrednio producentowi (a nie tylko Wykonawcy zamówienia).
- m) Bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon ....., e-mail na adres .... w języku Polskim oraz serwis WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją systemu bezpieczeństwa w trybie całodobowym w każdy dzień tygodnia.
- n) Możliwość pobrania bezpośrednio od producenta nowych wydań oprogramowania zgodnie z zapotrzebowaniem Zamawiającego, w ramach ogólnie dostępnej oferty producenta.
- 3) Zakres prac oraz termin ich wykonania będzie każdorazowo ustalany pomiędzy Zamawiającym i Wykonawcą w formie pisemnej lub za pośrednictwem poczty elektronicznej.
- 4) W okresie obowiązywania gwarancji, Wykonawca będzie świadczył usługi wsparcia przez wykwalifikowanych pracowników producenta lub autoryzowanego partnera producenta, posiadających ugruntowaną wiedzę potwierdzoną certyfikatami w zakresie systemu będącego przedmiotem Umowy.
- 5) Urządzenia muszą pracować po okresie licencyjnym z pełną funkcjonalnością każdego modułu bezpieczeństwa, z sygnaturami aktualnymi na ostatni dzień obowiązywania licencji.
- 6) Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
- 7) Jeżeli wykorzystanie którejkolwiek z wymienionych w OPZ funkcjonalności wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć.

#### 10. Testy wydajnościowe:

- 1) Zamawiający wymaga gotowości Wykonawcy do przeprowadzeniu testów w terminie nie dłuższym niż 8 dni roboczych liczonych od podpisania Umowy. Wykonawca w terminie wykonania testów musi dostarczyć kompletne środowisko testowe, w szczególności urządzenia i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów. Po wykonaniu testów Wykonawca zabierze dostarczone przez siebie na czas testów urządzenia. Testy mogą być prowadzone tylko i wyłącznie na terytorium Polski, w siedzibie Wykonawcy lub dowolnej lokalizacji wskazanej przez Zamawiającego (należącej do PGL LP).
- 2) Celem przeprowadzenia procedury testowej jest weryfikacja zgodności urządzeń i oprogramowania z wymaganiami zawartymi w OPZ.
- 3) Czas trwania testów nie może być dłuższy niż 8 godzin zegarowych.
- 4) Podczas testów Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane rozwiązanie posiada wymagane w OPZ funkcjonalności.

- 5) W sytuacji wystąpienia błędów oraz problemów uniemożliwiających prawidłowe przeprowadzenie testów. Wykonawca ma obowiązek podjęcia czynności zmierzających do ich usunięcia, w ramach czasu przewidzianego na testy. Zadania, które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane a test za niezaliczony. W przypadku niezaliczenia testów wydajnościowych w pierwszym terminie, Zamawiający dopuszcza jeden dzień roboczy na ponowne wykonanie testów przez Wykonawcę w kolejnym dniu roboczym. Negatywne zaliczenie testów w drugim terminie nie podlega ponownemu powtórzeniu, a test zostaje uznany ostatecznie za niezaliczony.
- 6) Testy przeprowadzone zostaną w języku Polskim, Zamawiający dopuszcza raporty generowane z urządzeń pomiarowych w języku Angielskim.
- 7) Testy muszą zostać wykonane dedykowanym urządzeniem dostarczonym przez Wykonawcę umożliwiającym wygenerowanie ruchu o wymaganej charakterystyce i wolumenie zgodnie ze specyfikacją minimalną przedstawioną w OPZ dla I,II grupy urządzeń firewall UTM. Urządzenie musi również umożliwiać generowanie próbek na podstawie pliku zawierającego podsłuchy lub skopiowany rzeczywisty ruch sieciowy.
- 8) Urządzenie generujące ruch musi mieć możliwość testowania parametrów wydajnościowych urządzeń sieciowych takich jak przełączniki, routery, firewall-e ngfw.
- 9) Urządzenie generujące ruch musi symulować pracę zarówno klienta jak i serwera dla testowanych parametrów wydajnościowych (odbiornik, nadajnik).
- 10) Urządzenie musi mieć możliwość wygenerowania ruchu o wolumenie większym, niż wymagany przez Zamawiającego.
- 11) Urządzenie powinno posiadać predefiniowane przez producenta próbki symulujące ruch generowany przez różnego rodzaju aplikacje, grupy aplikacji oraz protokoły np. usługi Microsoft Windows Update, Facebook, Microsoft Exchange, MS SQL, Microsoft Edge, LDAP, SMB, SMTP, DNS, HTTP oraz HTTPS itp.
  - a) Jeżeli urządzenie testujące dostarczone przez Wykonawcę nie posiada predefiniowanych próbek Zamawiający dopuszcza wykorzystanie próbki dostarczonej przez Wykonawcę z zastrzeżeniem, że próbka zostanie szczegółowo opisana.
  - b) Szczegółowe informacje dot. próbki oraz sama próbka zostanie przekazana Zamawiającemu razem z raportem końcowym przeprowadzonych testów.
- 12) Urządzenie testujące musi posiadać możliwość wygenerowania ruchu dla wybranych grup aplikacji, o określonym wolumenie i określonej liczbie symulowanych użytkowników.
- 13) Podczas procedury testowej na urządzeniach opisanych w OPZ z grupy I,II sprawdzona zostanie funkcjonalność modułów:
  - a) Rozpoznanie aplikacji – podczas testu urządzenie musi zidentyfikować aplikację generującą ruch. Potwierdzeniem zaliczenia testu będzie informacja w logu urządzenia testowanego z prawidłowo rozpoznaną aplikacją.
  - b) Rozpoznanie AntyVirus – podczas testu nastąpi próba przesłania zainfekowanego pliku za pomocą protokołu http oraz https (Zamawiający zaleca wykorzystanie próbki ze strony „<https://www.eicar.org/>” lub dostarczy przygotowaną wcześniej próbkę na prośbę Wykonawcy). Następnie test zostanie powtórzony z przesłaniem tego samego pliku poddanego kompresji \*.zip bez użycia hasła. Potwierdzeniem zaliczenia testu będzie informacja w logu urządzenia testowanego o zablokowanym ruchu zarówno dla pliku oryginalnego jak i skompresowanego.
  - c) Rozpoznanie IPS – Test polega na wygenerowaniu dowolnego zdarzenia rozpoznanego przez moduł IPS urządzenia testowanego. Potwierdzeniem zaliczenia będzie informacja w logu urządzenia.

- d) Wydajność ruchu Firewall z włączoną funkcją kontroli aplikacji (pakiet 64KB HTTP) zgodnie ze specyfikacją podaną w OPZ dla I,II grupy urządzeń. Zamawiający dopuszcza tolerancję błędu pomiarowego środowiska testującego wynoszącą +/- 5%. Potwierdzeniem zaliczenia testu będzie raport z generatora ruchu o przepływności nie mniejszej niż podana w OPZ z uwzględnieniem tolerancji błędu.
  - e) Wydajność ruchu typu Enterprise nie mniej niż zgodnie z podaną specyfikacją w OPZ dla I,II grupy urządzeń kontroli NGFW (Firewall, Application Control, IPS, antymalware) Potwierdzeniem zaliczenia testu będzie raport z generatora ruchu zawierający informacje o przepływności ruchu. Zamawiający dopuszcza tolerancję błędu wynoszącą +/- 5%.
  - f) Możliwość obsłużenia nowych sesji na sekundę zgodnie z podaną specyfikacją w OPZ dla I,II grupy urządzeń. Zamawiający dopuszcza tolerancję błędu pomiarowego środowiska testowego wynoszącą +/- 5%. Potwierdzeniem zaliczenia testu będzie raport z ruchu zawierający informację o liczbie nowych sesji na sekundę.
- 14) Po zakończeniu testów urządzenie musi wygenerować raport z wykonanego testu zawierający informację o:
- a) Wolumenie wygenerowanego ruchu dla badanych funkcjonalności;
  - b) Procentowym udziale poszczególnych aplikacji w wolumenie generowanego ruchu;
  - c) Liczba błędów w generowanym ruchu;
  - d) Liczbie wygenerowanych nowych sesji TCP na sekundę;
  - e) Raport z logów urządzeń testowanych z modułów IPS, Application Control, Firewall, AntyVirus;

#### **11. Testy akceptacyjne:**

- 1) Wykonawca opracuje w ramach Projektu techniczny Plan oraz Scenariusze testów akceptacyjnych.
- 2) Scenariusze testów akceptacyjnych muszą być tak przygotowane, aby mogły być wykonane również przez osoby niebiorące czynnego udziału we wdrożeniu urządzeń.
- 3) Wykonawca przeprowadzi w obecności przedstawicieli Zamawiającego Testy akceptacyjne dla Urządzeń Bezpieczeństwa dla wybranych jednostek z każdej grupy. Pozytywny wynik Testów akceptacyjnych dla każdej lokalizacji będzie stanowił podstawę do sporządzenia Protokołu Odbioru dla danej lokalizacji.
- 4) W pozostałych jednostkach testy akceptacyjne przeprowadzi Administrator Centralny, Regionalny lub Techniczny.
- 5) Po uruchomieniu wszystkich Urządzeń Bezpieczeństwa, Wykonawca przeprowadzi Testy akceptacyjne dla systemu CP. Pozytywny wynik Testów akceptacyjnych będzie podstawą do sporządzenia Dokumentacji powykonawczej.

#### **12. Dokumentacja powykonawcza:**

- 1) Dokumentacja powykonawcza musi objąć swym zakresem wszystkie czynności, które zostały przeprowadzone podczas wdrożenia i analizy, konfigurację urządzeń i systemu zarządzająco-raportującego, schemat logiczny i fizyczny połączeń.
- 2) Opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla Systemu (dziennych, tygodniowych, miesięcznych itp.) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa;

- 3) Opis zasad konserwacji i utrzymania Systemu takich jak informacja o okresowych zadaniach, które muszą być wykonane przez administratorów, np.: weryfikacja zajętości przestrzeni, konieczność wykonania analizy tabel, czyszczenia logów;

**13. Wymagania dotyczące przeprowadzenia szkolenia powdrożeniowego dla Administratorów Regionalnych:**

- 1) Wykonawca przeprowadzi szkolenie powdrożeniowe obejmujące zakresem, instalację, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu u Zamawiającego bezpieczeństwa firewall UTM zgodnie z następującymi wymaganiami:
  - a) Liczba uczestników – 19 osób;
  - b) Program szkolenia musi zawierać całość zagadnień obejmujących, administrowanie wdrożonym systemem oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie;
  - c) Szkolenie zostanie przeprowadzone i omówione na środowisku produkcyjnym w lokalizacjach wskazanych przez Zamawiającego;
  - d) Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.
  - e) Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.

**14. Wymagania dotyczące przeprowadzenia szkolenia certyfikowanego z obsługi i zarządzania urządzeniami klasy UTM producenta urządzeń dla Zespołu wdrożeniowego oraz wyznaczonych Administratorów Centralnych:**

1. Wykonawca zapewni po podpisaniu Umowy z Zamawiającym szkolenie lub szkolenia przez autoryzowany ośrodek obejmujące zakresem, instalację, konfigurację, zarządzanie rozwiązywanie problemów dostarczonego systemu bezpieczeństwa firewall UTM, które przeprowadzone zostanie zgodnie z następującymi wymaganiami:
  - a) Liczba uczestników – 5 osób;
  - b) Szkolenie zostanie przeprowadzone na środowisku szkoleniowym przygotowanym przez autoryzowany ośrodek poza siedzibą Zamawiającego na terenie Polski;
  - c) Program szkolenia musi zawierać całość zagadnień obejmujących instalację, konfigurację, administrowanie systemem oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie;
  - d) Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF;
  - e) Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim.
  - f) Wszyscy uczestnicy otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia;
2. Wykonawca zapewni każdemu uczestnikowi szkolenia samodzielne stanowisko pracy;
3. Na co najmniej 14 dni przed rozpoczęciem szkolenia Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:
  - a) Programy szkoleń zawierające szczegółowe informacje o zakresie i tematyce oraz rozkładzie zajęć dla poszczególnych szkoleń. Program szkolenia musi obejmować:
    - przybliżenie wszystkich funkcji realizowanych przez firewall ze szczegółowym wytłumaczeniem idei i sposobu działania

- przedstawienie sposobu konfiguracji (parametry, przypadki zastosowania) w.w. funkcji
  - przedstawienie narzędzi do monitorowania pracy firewalla
  - przedstawienie sposobów analizy logów i monitorowania stanu sieci oraz wykrytych zagrożeń
  - przedstawienie sposobu generowania raportów oraz tworzenia własnych szablonów raportów (np. z użycia wszystkich połączeń VPN przez pracowników)
  - omówienie procedury aktualizacji oprogramowania oraz archiwizacji (backup) konfiguracji
  - omówienie procedury "password recovery" oraz "firmware recovery"
  - omówienie administrowania urządzeniami w tym konfiguracji i monitorowanie analizy zdarzeń oraz zarządzanie incydentami dla urządzeń firewall UTM za pomocą centralnej konsoli zarządzania i logowania;
  - omówienie procedury wymiany uszkodzonego urządzenia na posiadane urządzenie „sperowe” wraz z przeniesieniem wymaganej konfiguracji.
  - przedstawienie innych istotnych informacji dla administratora sieci.;
- b) Metodę oraz formę prowadzenia szkoleń;
  - c) Listę wykładowców i informacje o wykładowcach prowadzących poszczególne szkolenia.
4. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkoleń;
  5. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:
    - a) Materiały szkoleniowe;
    - b) Ankiety oceny szkoleń;
    - c) Listę obecności;
  6. Listę wydanych Zaświadczeń i komplet imiennych zaświadczeń (certyfikatów) dla wszystkich uczestników, którzy ukończą szkolenie .