**Załącznik nr 2**

Numer sprawy: PK XII BIA 0412.11.2018.8

1. **Przełącznik sieciowy SAN TYP 1 Liczba sztuk: 4**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. |
| W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |
| Przełącznik FC musi być wyposażony, w co najmniej 12 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s z możliwością rozbudowy do 24 portów FC 16Gb. |
| Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC |
| Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 384 Gb/s end-to-end. |
| Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 800ns. |
| Rodzaj obsługiwanych portów, co najmniej: E oraz F. |
| Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| Przełącznik FC posiadać nadmiarowy zasilacz i wentylator, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika. |
| Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. |
| Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |
| Przełącznik FC musi mieć możliwość konfiguracji przez:   1. polecenia tekstowe w interfejsie znakowym konsoli terminala 2. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. |
| Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:   1. logowanie zdarzeń poprzez mechanizm „syslog”, 2. FCping 3. FC traceroute 4. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika |
| Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s. |
| Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet. |
| Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
| Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. |
| Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. |
| Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. |
| Przełącznik FC musi zapewnić możliwość przydzielenia, co najmniej 7900 tzw. buffer credits do pojedynczego portu FC przełącznika |

1. **Przełącznik sieciowy SAN TYP 2 Liczba sztuk: 6**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. |
| W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |
| Przełącznik FC musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone wkładkami SFP 16Gb/s. |
| Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC |
| Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 384 Gb/s end-to-end. |
| Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 800ns. |
| Rodzaj obsługiwanych portów, co najmniej: E oraz F. |
| Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| Przełącznik FC posiadać nadmiarowy zasilacz i wentylator, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika. |
| Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. |
| Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |
| Przełącznik FC musi mieć możliwość konfiguracji przez:   1. polecenia tekstowe w interfejsie znakowym konsoli terminala 2. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. |
| Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:   1. logowanie zdarzeń poprzez mechanizm „syslog”, 2. FCping 3. FC traceroute 4. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika |
| Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s. |
| Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet. |
| Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
| Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. |
| Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. |
| Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. |
| Przełącznik FC musi zapewnić możliwość przydzielenia, co najmniej 7900 tzw. buffer credits do pojedynczego portu FC przełącznika |

1. **Przełącznik sieciowy SAN TYP 3 Liczba sztuk: 2**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. |
| W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |
| Przełącznik FC musi być wyposażony, w co najmniej 96 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s. |
| Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC |
| Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 3072 Gb/s end-to-end full duplex. |
| Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 800ns. |
| Rodzaj obsługiwanych portów, co najmniej: E oraz F. |
| Przełącznik FC musi mieć wysokość maksymalnie 2 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| Przełącznik FC posiadać nadmiarowy zasilacz i wentylator, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika. |
| Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. |
| Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |
| Przełącznik FC musi mieć możliwość konfiguracji przez:   1. polecenia tekstowe w interfejsie znakowym konsoli terminala 2. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. |
| Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:   1. logowanie zdarzeń poprzez mechanizm „syslog”, 2. FCping 3. FC traceroute 4. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika |
| Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s. |
| Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet. |
| Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
| Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. |
| Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s half duplex dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. |
| Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. |
| Przełącznik FC musi zapewnić możliwość przydzielenia, co najmniej 7900 tzw. buffer credits do pojedynczego portu FC przełącznika |

1. **Urządzenie bezpieczeństwa sieciowego TYP 1 Liczba sztuk: 6**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Urządzenie bezpieczeństwa sieciowego firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi być wyposażone w co najmniej 4 porty Ethernet 100M/1000M, 16 portów 1G/10G SFP/SFP+, 4 porty 40G QSFP+.  Urządzenie bezpieczeństwa wyposażone w minimum 4 wkładeki SFP+ 10GbBaseSR. |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| Pojedyncza, logiczna instacja systemu będzie pozwalać na jednoczesną pracę w trybie routera ( tzn. w warstwie 3 modelu OSI) oraz w trybie transparentnym. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać nie mniej niż 25 wirtualnych systemów z możliwością rozbudowy do 125 za pomocą dodatkowych licencji |
| Urządzenie bezpieczeństwa sieciowego firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| Urządzenie bezpieczeństwa sieciowego firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury |
| Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 9 Gbit/s. |
| Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM) |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| Urządzenie bezpieczeństwa sieciowego firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
| Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| Urządzenie bezpieczeństwa sieciowego firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |

1. **Urządzenie bezpieczeństwa sieciowego TYP 2 Liczba sztuk: 4**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Urządzenie bezpieczeństwa sieciowego firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 35 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 18 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 8 000 000 jednoczesnych połączeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi być wyposażony w co najmniej 4 porty Ethernet 100M/1000M, 16 portów 1G/10G SFP/SFP+, 4 porty 40G/100G QSFP28.  Urządzenie bezpieczeństwa wyposażone w minimum 4 wkładki SFP+ 10GbBaseSR |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| Pojedyncza, logiczna instacja systemu będzie pozwalać na jednoczesną pracę w trybie routera ( tzn. w warstwie 3 modelu OSI) oraz w trybie transparentnym. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać nie mniej niż 25 wirtualnych systemów z możliwością rozbudowy do 125 za pomocą dodatkowych licencji |
| Urządzenie bezpieczeństwa sieciowego firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| Urządzenie bezpieczeństwa sieciowego firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury |
| Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 18 Gbit/s. |
| Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM) |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| Urządzenie bezpieczeństwa sieciowego firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
| Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| Urządzenie bezpieczeństwa sieciowego firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |

1. **Urządzenie bezpieczeństwa sieciowego TYP 3 Liczba sztuk: 4**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Urządzenie bezpieczeństwa sieciowego firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 1.9 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 700Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 190 000 jednoczesnych połączeń. |
| System zabezpieczeń firewall musi być wyposażony w co najmniej 8 portów Ethernet 100M/1G, 4 porty 10Gbps SFP+. |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |
| Pojedyncza, logiczna instacja systemu będzie pozwalać na jednoczesną pracę w trybie routera ( tzn. w warstwie 3 modelu OSI) oraz w trybie transparentnym. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. |
| Urządzenie bezpieczeństwa sieciowego firewall musi obsługiwać nie mniej niż 25 wirtualnych systemów z możliwością rozbudowy do 125 za pomocą dodatkowych licencji |
| Urządzenie bezpieczeństwa sieciowego firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |
| Urządzenie bezpieczeństwa sieciowego firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |
| Urządzenie bezpieczeństwa sieciowego firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury |
| Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 1.9 Gbit/s. |
| Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM) |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |
| Urządzenie bezpieczeństwa sieciowego firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |
| Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |
| Urządzenie bezpieczeństwa sieciowego firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |
| Urządzenie bezpieczeństwa sieciowego firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |
| Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| Urządzenie bezpieczeństwa sieciowego firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |
| Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |
| Urządzenie bezpieczeństwa sieciowego firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS |
| Urządzenie bezpieczeństwa sieciowego firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |

1. **System zarządzania firewallami Liczba sztuk: 1**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| System zarządzania, logowania i raportowania musi obsługiwać min. **25** firewalli i min. **250** logicznych systemów. |
| System musi zarządzać wszystkimi dostarczanymi Systemami zabezpieczeń firewall |
| System zarządzania, logowania i raportowania musi zapewniać przestrzeń dyskową o pojemności nie mniejszej niż 24 TB. |
| System zarządzania, logowania i raportowania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie. |
| System zarządzania, logowania i raportowania musi posiadać taki sam Graficzny Interfejs Użytkownika jak zarządzane firewalle. |
| System zarządzania, logowania i raportowania musi umożliwiać import obecnej konfiguracji używanych firewalli. |
| System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. |
| System zarządzania, logowania i raportowania musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli. |
| System zarządzania, logowania i raportowania musi umożliwiać łatwe przeszukiwanie skorelowanych logów zebranych z zarządzanych firewalli. |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”. |
| System zarządzania, logowania i raportowania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) i globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). |
| System zarządzania, logowania i raportowania musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów). |
| System zarządzania, logowania i raportowania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. |
| System zarządzania, logowania i raportowania musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. |
| System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur. |
| System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek. |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli. |
| System zarządzania, logowania i raportowania musi pozwalać na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu konsoli zarządzającej. |
| System zarządzania, logowania i raportowania musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi. |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne). |
| System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. |
| System zarządzania, logowania i raportowania musi informować o zmianach konfiguracji systemu. |
| System zarządzania, logowania i raportowania musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem. |
| System zarządzania, logowania i raportowania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów. |
| System zarządzania, logowania i raportowania musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał iż nowe urządzenie zastępuje urządzenie uszkodzone. |
| System zarządzania, logowania i raportowania musi być dostarczony jako maszyna wirtualna. |

1. **Przełączniki LAN TYP 1 Liczba sztuk: 5**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Przełącznik o budowie modularnej pozwalającej na instalację minimum: 192 portów 1Gbps, 192 portów 10Gbps SFP+, 192 portów Ethernet 10-gigabitowych, 144 porty 40Gbps, 144 portów 100Gbps lub ich kombinacji. |
| 1. Typ i liczba portów: 2. Minimum 96 portów 10GbE SFP+ umieszczonych z przodu obudowy, dla zapewnienia redundancji porty te muszą być rozdzielone na co najmniej dwa różne moduły 3. Minimum 40 portów 40GbE/100GbE QSFP28 umieszczonych z przodu obudowy, dla zapewnienia redundancji porty te muszą być rozdzielone na co najmniej dwa różne moduły 4. Minimum 36 portów 40GbE QSFP+ umieszczonych z przodu obudowy, dla zapewnienia redundancji porty te muszą być rozdzielone na co najmniej dwa różne moduły   Przełącznik wyposażony w:   1. minimum 30 wkładek SFP+ 10GbBaseSR 2. minimum 28 wkładek QSFP+ 40GbBaseSR4 3. minimum 2 kable typu DAC QSFP28 działające z prędkością 100GbE o długości minimum 3 metry |
| Redundantne moduły zarządzające wyposażone w minimum 1GB pamięci stałej (typu Flash) oraz minimum 4GB pamięci operacyjnej (typu RAM) na każdym z modułów |
| Redundantne moduły przełączające (fabric) zapewniające co najmniej redundancję typu N+1 i pozwalające na przełączanie z pełną prędkością (tzw. wire-speed) dla wszystkich wymaganych portów przełącznika dla pakietów 128 bajtowych |
| Wielkość bufora pakietów (packet buffer): minimum 4GB na każdą kartę liniową  Wbudowany, dodatkowy, dedykowany port Ethernet RJ-45 do zarządzania poza pasmem - out of band management, na każdym module zarządzającym |
| Port konsoli RS232 ze złączem DB9 lub RJ45, na każdym module zarządzającym |
| Przełączanie w warstwie 2 i 3 modelu OSI |
| Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów), dopuszcza się moduły wentylatorów zintegrowane z kartami, pod warunkiem zachowania ich redundancji |
| Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. |
| Wewnętrzne, modularne, zasilacze AC zapewniające pełną redundancję zasilania, typu N+N, wymieniane podczas pracy urządzenia. |
| Wielkość tablicy routingu: minimum 120000 wpisów |
| Tablica adresów MAC o wielkości minimum 360000 pozycji |
| Funkcja łączenia w stos grupy, co najmniej 2 przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie, co najmniej z perspektywy realizacji link aggregation w ramach różnych przełączników będących w stosie |
| Obsługa ramek Jumbo o wielkości minimum 9216B |
| Obsługa Quality of Service |
| Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) |
| Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ |
| Routing IPv4 – statyczny i dynamiczny (min. RIP, OSFP, ISIS, BGP) |
| Obsługa tunelowania GRE |
| Obsługa ECMP (Equal Cost Multi Path) |
| Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.  Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia |
| Obsługa standardu 802.1p, 8 kolejek wyjściowych na każdym porcie |
| Obsługa Network Time Protocol (NTP) |
| Obsługa protokołu OpenFlow |
| Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). |
| Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji) |
| Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian |
| Wysokość w szafie 19” nie więcej niż 7U. Głębokość nie większa niż 90cm |
| Przełączniki sieciowe muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie może znajdować się na liście „end-of-sale” oraz „end-of-support” producenta. |
| Przełączniki sieciowe muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej. |
| Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. |

1. **Przełączniki LAN TYP 2 Liczba sztuk: 14**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Minimum 48 portów 10/100/1000BaseT |
| Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) oraz Gigabitowych (SFP), umieszczonych z przodu obudowy.  Każdy przełącznik wyposażony w minimum dwie wkładki SFP+ 10GbBaseSR |
| Slot rozszerzeń pozwalający na rozbudowę o dodatkowe dwa porty 10Gb SFP+ |
| Dwa modularne, wewnętrzne zasilacze prądu zmiennego. Zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco |
| Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa, niezależne, moduły wentylatorów) |
| Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. |
| Wydajność: minimum 216Gb/s (prędkość przełączania „wirespeed” dla każdego portu przełącznika) |
| Przepustowość: minimum 162Mp/s |
| Przełączanie w warstwie 2 i 3 modelu OSI |
| Wielkość tablicy routingu: minimum 32000 wpisów |
| Tablica adresów MAC o wielkości min. 32000 pozycji |
| Minimum 2GB pamięci operacyjnej |
| Minimum 512MB pamięci typu Flash |
| Minimum 4MB bufora pamięci pakietów |
| Port USB pozwalający na kopiowanie plików (w tym pliki konfiguracyjne i z oprogramowaniem przełącznika) z i do urządzenia |
| Funkcja agregacji fizycznych interfejsów z wykorzystaniem protokołu LACP (802.3ad). |
| Funkcja łączenia w stos grupy, co najmniej 2 przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie, co najmniej z perspektywy realizacji link aggregation w ramach różnych przełączników będących w stosie |
| Obsługa ramek Jumbo (minimum do 9216B) |
| Obsługa IEEE 802.1s Multiple SpanningTree / MSTP (minimum 64 instancje) oraz IEEE 802.1w Rapid Spanning Tree Protocol |
| Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ |
| Routing IPv4 – statyczny i dynamiczny (min. RIP, OSFP, ISIS, BGP) |
| Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.  Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia |
| Obsługa standardu 802.1p |
| Obsługa NETCONF lub OpenConfig |
| Network Time Protocol (NTP) |
| Obsługa protokołu OpenFlow |
| Obsługa 802.3x flow control |
| Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). |
| Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). |
| Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. |
| Wysokość w szafie rack 19” – 1U. |
| Przełączniki sieciowe muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej. |

1. **Przełączniki LAN TYP 3 Liczba sztuk: 20**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Typ i liczba portów:   1. Minimum 48 portów obsługujących prędkość co najmniej 10GbE w standardzie SFP+ lub SFP28 umieszczonych z przodu obudowy 2. Minimum 6 portów 40GbE/100GbE QSFP28 umieszczonych z przodu obudowy 3. Każdy przełącznik wyposażony w minimum 24 wkładki SFP+ 10GbBaseSR 4. Każdy przełącznik wyposażony w minimum 4 wkładki QSFP+ działające na dwóch włóknach światłowodu wielomodowego na odległość co najmniej 100m. |
| Port konsoli RS232 ze złączem DB9 lub RJ45 |
| Port USB 2.0 |
| Wydajność: minimum 2160 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) |
| Przepustowość: minimum 1600 Mp/s |
| Przełączanie w warstwie 2 i 3 modelu OSI |
| Opóźnienie przełączania transmisji 10GbE dla pakietów 64 bajtowych poniżej 3µs |
| Mechanizmy przełączania: store and forward |
| Wielkość bufora pakietów (packet buffer): minimum 12MB |
| Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów) |
| Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza. |
| Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. |
| Wielkość tablicy routingu: minimum 120000 wpisów |
| Funkcja łączenia w stos grupy, co najmniej 2 przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie, co najmniej z perspektywy realizacji link aggregation w ramach różnych przełączników będących w stosie |
| Tablica adresów MAC o wielkości minimum 128000 pozycji |
| Obsługa ramek Jumbo o wielkości minimum 9216B |
| Obsługa Quality of Service |
| Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) |
| Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ |
| Routing IPv4 – statyczny i dynamiczny (min. RIP, OSFP, ISIS, BGP) |
| Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia |
| Obsługa standardu 802.1p, 8 kolejek wyjściowych na każdym porcie |
| Funkcja zmiany wartości pola DSCP i wartości priorytetu 802.1p |
| Funkcje mirroringu: 1 to 1 Port mirroring, Many to 1 port mirroring, Flow mirroring, L2 remote mirroring, L3 remote mirroring |
| Zarządzanie poprzez port konsoli, SNMP v1, 2c i 3, SSH v2 |
| Obsługa Syslog |
| Obsługa Network Configuration Protocol (NETCONF) lub OpenConfig |
| Obsługa Network Time Protocol (NTP) |
| Obsługa protokołu OpenFlow |
| Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania). |
| Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji). |
| Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. |
| Wysokość w szafie 19” – 1U. |
| Przełączniki sieciowe muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej. |

1. **Urządzenie loadbalancer TYP 1 Liczba sztuk: 3**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

|  |  |
| --- | --- |
| **Opis wymagań minimalnych** | |
| Pamięć | Nie mniej niż 48GB |
| Dysk twardy | Jeden dysk SSD o pojemności nie mniejszej niż 480GB |
| Przepływność dla warstwy 4 | Nie mniej niż 60 Gbps |
| Przepływność dla warstwy 7 | Nie mniej niż 35 Gbps |
| Przepustowość wewnętrznej magistrali | Nie mniej niż 640 Gbps |
| Ilość jednocześnie obsługiwanych połączeń | Nie mniej niż 40 miliony |
| Ilość transakcji SSL na sekundę dla klucza o długości 2048 | Nie mniej niż 35 tysięcy |
| Ilość transakcji SSL na sekundę dla szyfrowania ECC (ECDHE-ECDSA-AES128-SHA256) | Nie mniej niż 20 tysięcy |
| Przepływność ruchu szyfrowanego | Nie mniej niż 20 Gbps |
| Ilość połączeń na sekundę w warstwie 4 | Nie mniej niż 800 tysięcy |
| Kompresja sprzętowa | Nie mniej niż 15 Gbps |
| Sprzętowa ochrona DDoS | Nie mniej niż 50 milionów SYN cookies na sekundę |
| Gęstość interfejsów | Nie mniej niż osiem interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX) lub SFP+ 10G (SR lub LR), nie mniej niż cztery interfejsy z możliwością obsadzenia wkładkami 40Gb QSFP+, oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB  Urządzenie wyposażone w minimum 8 wkładek SFP+ 10GbBaseSR |
| Zarządzanie | Panel i wyświetlacz LCD (dotykowy) z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu urządzenia, wyświetlania informacji o systemie  Funkcjonalność „Always On Management” |
| Obudowa | Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 1 U |
| Zasilanie | Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC |
| Urządzenie fizyczne (appliance) musi realizować co najmniej następujące funkcje:   1. Rozkład ruchu pomiędzy serwerami aplikacji Web 2. Selektywny http caching 3. Selektywna kompresja danych 4. Terminowanie sesji SSL | |
| Urządzenie typu loadbalancer musi posiadać co najmniej następujące metody równoważenia obciążenia:   1. Cykliczna 2. Ważona 3. Najmniejsza liczba połączeń 4. Najszybsza odpowiedź serwera 5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera 6. Dynamicznie ważona oparta na SNMP/WMI 7. Definiowana na podstawie grupy priorytetów dla serwerów | |
| Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:   1. Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów 2. Obsługa protokołów: http, tcp, xml, rtsp, sip 3. Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS | |
| Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w system interfejsu graficznego. | |
| Rozwiązanie musi obsłużyć sprzętowo minimum 50 milionów SYN cookies na sekundę | |
| Urządzenie musi posiadać co najmniej następujące interfejsy administracyjne:   1. GUI przy wykorzystaniu protokołu https 2. Zarządzanie poprzez SSH 3. Zarządzanie poprzez SOAP-SSL 4. Zarządzanie poprzez API REST | |
| Urządzenie musi świadczyć, co najmniej następujące usługi w warstwach 4-7:   1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http 2. Ukrywanie zasobów 3. Zmiana odpowiedzi serwera 4. Przepisywanie odpowiedzi (response rewriting) 5. Ochrona przed atakami typu DoS/DDoS 6. Ochrona przed atakami typu SYN Flood 7. Multipleksowanie połączeń http | |

1. **Urządzenie loadbalancer TYP 2 Liczba sztuk: 5**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

|  |  |
| --- | --- |
| **Opis wymagań minimalnych** | |
| Pamięć | Nie mniej niż 48GB |
| Dysk twardy | Jeden dysk SSD o pojemności nie mniejszej niż 480GB |
| Przepływność dla warstwy 4 | Nie mniej niż 60 Gbps |
| Przepływność dla warstwy 7 | Nie mniej niż 35 Gbps |
| Przepustowość wewnętrznej magistrali | Nie mniej niż 640 Gbps |
| Ilość jednocześnie obsługiwanych połączeń | Nie mniej niż 40 miliony |
| Ilość transakcji SSL na sekundę dla klucza o długości 2048 | Nie mniej niż 35 tysięcy |
| Ilość transakcji SSL na sekundę dla szyfrowania ECC (ECDHE-ECDSA-AES128-SHA256) | Nie mniej niż 20 tysięcy |
| Przepływność ruchu szyfrowanego | Nie mniej niż 20 Gbps |
| Ilość połączeń na sekundę w warstwie 4 | Nie mniej niż 800 tysięcy |
| Kompresja sprzętowa | Nie mniej niż 20 Gbps |
| Sprzętowa ochrona DDoS | Nie mniej niż 50 milionów SYN cookies na sekundę |
| Gęstość interfejsów | Nie mniej niż osiem interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX) lub SFP+ 10G (SR lub LR), nie mniej niż cztery interfejsy z możliwością obsadzenia wkładkami 40Gb QSFP+, oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB  Urządzenie wyposażone w minimum 8 wkładek SFP+ 10GbBaseSR |
| Zarządzanie | Panel i wyświetlacz LCD (dotykowy) z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu urządzenia, wyświetlania informacji o systemie  Funkcjonalność „Always On Management” |
| Obudowa | Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 1 U |
| Zasilanie | Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC |
| Urządzenie fizyczne ( appliance) musi realizować co najmniej następujące funkcje:   1. Rozkład ruchu pomiędzy serwerami aplikacji Web 2. Selektywny http caching 3. Selektywna kompresja danych 4. Terminowanie sesji SSL 5. Ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall) | |
| Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia | |
| Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej | |
| Urządzenie musi posiadać co najmniej następujące metody równoważenia obciążenia:   1. Cykliczna 2. Ważona 3. Najmniejsza liczba połączeń 4. Najszybsza odpowiedź serwera 5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera 6. Dynamicznie ważona oparta na SNMP/WMI 7. Definiowana na podstawie grupy priorytetów dla serwerów | |
| Funkcjonalność lokalnego równoważenia obciążenia   1. Wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego 2. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera 3. Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług 4. Obsługiwane mechanizmy przywiązywania sesji: cookie, adres źródłowy, adres docelowy, SSL ID ,JSESSIONID 5. Wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP | |
| Optymalizacja i akceleracja aplikacji   1. Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: 2. LAN 3. WAN 4. CELL (komórkowy) 5. Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta. 6. Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control) 7. Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP 8. Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od: 9. Listy dozwolonych URI 10. Listy wykluczonych URI 11. Listy kompresowalnych Content-Type 12. Listy wykluczonych Content-Type | |
| WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:   1. wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a. 2. typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT) 3. przejścia pomiędzy URL-ami (servletami) 4. dopuszczalne metody http, 5. dopuszczalne cookie, 6. dopuszczalne parametry w polityce, 7. parametry dynamiczne, 8. typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany) oraz dopuszczalne parametry w danym serwlecie 9. długość zapytań 10. nazwy hosta 11. wystąpień i długość parametrów (per każdy parametr) 12. wystąpień i długości nagłówków 13. wystąpień i długości cookies 14. oczekiwanych typów znaków per każdy parametr 15. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku 16. URL-i podatnych na CSRF | |
| WAF musi posiadać mechanizmy ochrony przed atakami:   1. SQL Injection, 2. Cross-Site Scripting, 3. Cross-Site Request Forgery, 4. Session hijacking, 5. Command Injection, 6. Cookie/Session Poisoning, 7. Parameter/Form Tampering, 8. Forceful Browsing, 9. Brute Force Login, 10. Web Scraping 11. Cookie manipulation/poisoning 12. Dynamic Parameter tampering 13. Buffer Overflow 14. Stealth Commanding 15. Unused HTTP Methods 16. Malicious File Uploads 17. Hidden Field Manipulation | |
| Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do :   1. Bazy danych : Microsoft SQL, ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2 2. Urządzenie typu loadbalancer Operacyjny : Windows, Linux, UNIX 3. Język aplikacji, frameworki : ASP, ASP .NET, PHP, Java, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Java Servlets/JSP, Lotus Domino, Macromedia ColdFusion, JRun, Outlook Web Access, SSI, WebDAV, JQuery, PHP, SSI, WebDAV, jQuery 4. Serwer WWW : Apache, Apache Tomcat, Microsoft IIS, serwerów proxy. | |
| WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http) | |
| WAF musi blokować ataki typu Slow Loris | |
| WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:   1. Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania 2. Mechanizmu browser fingerprinting , w celu wykrycia tzw. headless broser 3. Sygnatur botów 4. Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik). | |
| Moduł ochrony przed DDoS powinien wykrywać ataki per:   1. Source IP, 2. Obszar geolokacyjny, 3. URL, 4. Globalnie - website | |
| WAF musi posiadać możliwość ochrony komunikacji XML poprzez:   1. walidację Schema/WSDL, 2. wybór dozwolonych metod SOAP, 3. szyfrację /deszyfrację fragmentów wiadomości SOAP, 4. Wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie), 5. Definiowanie możliwości użycia załączników wiadomości SOAP, 6. Włączanie/wyłączanie podążania za odnośnikami do schematów SOAP, 7. Walidację SOAP Action Header, 8. Włączanie/wyłączanie możliwości użycia DTD 9. Włączanie/wyłączanie możliwości użycia zewnętrznych referencji 10. Włączanie/wyłączanie możliwości użycia początkowych białych znaków 11. Włączanie/wyłączanie możliwości użycia numerycznych nazw 12. Włączanie/wyłączanie możliwości użycia Processing Instructions 13. Włączanie/wyłączanie możliwości użycia CDATA 14. Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace 15. Ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów 16. Definicję dopuszczalnych znaków 17. Definicję sygnatur. | |
| Musi istnieć możliwość rozszerzenia funkcji WAF o dodatkowy serwis, sprawdzający reputację adresów IP dostających się do chronionej aplikacji. Serwis reputacyjny powinien być dostępny poprzez dodanie licencji, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania. | |
| Rozwiązanie musi obsłużyć sprzętowo minimum 50 milionów SYN cookies na sekundę | |
| Urządzenie typu loadbalancer musi posiadać co najmniej następujące interfejsy administracyjne:   1. GUI przy wykorzystaniu protokołu https 2. Zarządzanie poprzez SSH 3. Zarządzanie poprzez SOAP-SSL 4. Zarządzanie poprzez API REST | |
| Urządzenie musi świadczyć, co najmniej następujące usługi w warstwach 4-7:   1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http 2. Ukrywanie zasobów 3. Zmiana odpowiedzi serwera 4. Przepisywanie odpowiedzi (response rewriting) 5. Ochrona przed atakami typu DoS/DDoS 6. Ochrona przed atakami typu SYN Flood 7. Multipleksowanie połączeń http | |

1. **Urządzenie typu SIEM Liczba sztuk: 1**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

|  |
| --- |
| **Opis wymagań minimalnych** |
| Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności zarówno z użyciem wersji appliance (sprzętowej) jak i softwareowej (maszyna wirtualna). |
| System musi zapewniać obsługę i wydajność na poziomie minimum 2500 zdarzeń na sekundę (EPS, Events per Second) oraz 100 000 przepływów na minutę (Flow per Minute). Zamawiający szacuje liczbę urządzeń fizycznych będących pod monitoringiem systemu SIEM na poziomie do 100 sztuk. W przypadku uwzględnienia hostów wirtualnych, liczba ta może wzrosnąć trzykrotnie. |
| System musi umożliwiać integrację z innymi rozwiązaniami bezpieczeństwa (network intelligence, incident forensic, risk management, etc.) do czego niezbędne są następujące mechanizmy:   1. zdolność do przekazywania dalej logów i danych o aktywności sieciowej z SIEM do innych rozwiązań, zdolność do zbierania logów z dowolnych produktów bezpieczeństwa, w celu ich przechowywania, normalizacji i analizy, 2. zdolność do integracji z rozwiązaniami potrafiącymi dokonać rejestracji pakietów sieciowych powiązanych z zarejestrowanymi zdarzeniami (np. urządzenia IPS), wraz z możliwością przekazywania dalej zgromadzonych danych, 3. zdolność adaptacji/rekonfiguracji/przystosowania SIEM do współpracy z różnymi rozwiązaniami bezpieczeństwa poprzez edycję ustawień i/lub skrypty, 4. zdolność do przekazania dalej skorelowanej informacji o wykrytym ataku lub działaniu niepożądanym do innych rozwiązań bezpieczeństwa i/lub urządzeń sieciowych. |
| Rozwiązanie musi umożliwiać dostosowanie systemu do indywidualnych potrzeb Zamawiającego, szczególnie w zakresie:   1. możliwości edycji i dowolnego konfigurowania widoków danych bezpieczeństwa na pulpitach (dashboards), 2. możliwości edycji, dowolnego konfigurowania i tworzenia nowych reguł korelacji zdarzeń, tak aby możliwym było dopasowanie działania do konkretnych przypadków użycia, zarządzania ryzykiem, monitorowania zgodności z wytycznymi i przepisami, 3. możliwość edycji, dowolnego konfigurowania i tworzenia nowych szablonów raportów, 4. możliwość tworzenia, konfigurowania i zapisywania zapytań, wyszukiwań, widoków wykorzystywanych przy analizie, w celu późniejszej analizy lub ponownego wykorzystania raz użytych składni i założeń. |
| Rozwiązanie musi zapewniać elastyczną skalowalność, tak w zakresie rozbudowy wydajnościowej pod kątem zwiększenia liczby obsługiwanych zdarzeń (EPS) czy terminu i liczby ich składowania, jak również pod kątem rozbudowy geograficznej systemu, poprzez wyniesione moduły agregacji i retencji danych (zdarzenia, przepływy sieciowe, etc.), zdalne dostępy do konsoli na różnym poziomie dostępu, przy jednoczesnym zachowaniu centralnego: zarządzania, korelacji, zależności czy zakresie wyszukiwania i raportowania. Wymaganie w zakresie zbierania danych dotyczy mechanizmów agentowych i bez-agentowych. |
| Rozwiązanie musi obsługiwać rozproszone źródła danych (zdarzenia, aktywność sieciowa) w taki sposób, aby wszystkie zebrane dane były dostępne z jednego interfejsu użytkownika. |
| Rozwiązanie musi zapewniać integralność zebranych informacji, chroniąc zgromadzone i przetwarzane dane źródłowe przed manipulacją i utratą. |
| Rozwiązanie musi umożliwiać rozproszoną korelację zdarzeń, tzn. musi potrafić skorelować np. wielowątkowe zdarzenia z różną liczbą zdarzeń z różnych źródeł i mechanizmów zbierania danych. Dane podlegające globalnej korelacji mogą pochodzić zarówno z dowolnych modułów zbierania danych (collectors) jak i wyników innych mechanizmów korelacyjnych. Pożądaną funkcjonalnością jest możliwość zastosowania zbudowanej reguły korelacji globalnie i lokalnie. |
| Rozwiązanie musi umożliwiać tagowanie/klasyfikowanie zdarzeń, w celu późniejszego szybszego wyszukiwania, korelacji, raportowania. Mechanizm tagowania/klasyfikacji prócz wbudowanych zasad, musi umożliwiać ustalanie własnych zasad użytkownika systemu. |
| Rozwiązanie musi zapewniać przejrzystość w zakresie realizowanych funkcji zbierania, agregacji, sortowania, filtrowania czy korelacji danych, we wszystkich komponentach, również w sytuacji ich geograficznego lub modułowego rozproszenia. |
| Rozwiązanie powinno umożliwiać wielowątkowość w zakresie obsługi różnych domen lub środowisk (różnych obsługiwanych systemów/klientów przez jedna instancję SIEM), w których mogą wystąpić takie same adresy IP, nazwy hostów, etc. np,: poprzez odpowiednie tagowanie lub oznaczanie pochodzenia zgromadzonych zdarzeń, wraz z zachowaniem możliwości ich niezależnego (one domain) lub całościowego (cross domain) korelowania w systemie. |
| Rozwiązanie musi wspierać mechanizm „master console" (Jedna konsola dla wielu instancji SIEM) |
| Rozwiązanie musi umożliwiać centralne zarządzanie wszystkimi komponentami systemu oraz wszystkimi funkcjami administracyjnymi, z jednej webowej konsoli zarządzającej, |
| Rozwiązanie musi umożliwiać takie zarządzanie uprawnieniami, aby możliwe było ograniczenie dostępu do danych dotyczących systemu i/lub konkretnego środowiska/domeny (np. poprzez ograniczenie dostępu do danych z konkretnego kolektora) dla wybranych użytkowników systemu i różnych poziomów funkcjonalności - zgodnie z modelem RBAC. |
| Rozwiązanie musi posiadać takie mechanizmy zarządzania uprawnieniami, aby możliwe było przez administratora stworzenie i definiowanie ról/grup/użytkowników z dostępem opartym o model RBAC. W szczególności chodzi o zdolność mechanizmów bezpieczeństwa systemu do indywidualnego nadawania lub ograniczania uprawnień poszczególnym użytkownikom i/lub grupom/rolom w zakresie określonych funkcji rozwiązania (administracja, raportowanie, filtrowanie zdarzeń, korelacja, podgląd pulpitów, etc.). |
| Rozwiązanie powinno posiadać mechanizm ukrywania (obfuskacji) danych, wraz z możliwością wskazania jakie dane powinny być ukrywane. |
| Rozwiązanie powinno zachować rozpoznawalność aktywów nawet w przypadku zmiany adresu IP (baza aktywów). |
| Rozwiązanie musi umożliwiać tworzenie niezależnych i niedostępnych dla wszystkich pulpitów z widokami dla specjalnych działań np. SOC, NOC. Takie pulpity powinny być widoczne tylko dla wybranych użytkowników i/lub ról/grup użytkowników, poprzez niezależną konsolę webową. |
| Rozwiązanie musi umożliwiać modyfikację ustawień portów komunikacyjnych dla poszczególnych modułów systemu i zbierania danych. |
| Rozwiązanie musi umożliwiać szyfrowanie komunikacji pomiędzy poszczególnymi modułami systemu i zbierania danych. |
| Rozwiązanie musi umożliwiać integrację z zewnętrznymi dostawcami mechanizmów uwierzytelniania (LDAP, AD, RADIUS, etc...) dla operatorów i administratorów systemu. |
| Rozwiązanie powinno posiadać wsparcie producenta, ale też wsparcie w formie dostępnego forum wymiany wiedzy/doświadczeń dotyczące produktu, które zostanie udostępnione bez limitu operatorom i administratorom systemu. |
| System powinien umożliwiać zwiększenie możliwości operacyjnych np. poprzez dodanie dodatkowych licencji, bez potrzeby zwiększania liczby fizycznych komponentów systemu. |
| Rozwiązanie powinno posiadać mechanizmy usprawniające jego wykorzystanie i wdrożenie, np.:   1. automatyczne wykrywanie źródeł logów 2. automatyczne wykrywanie aplikacji 3. automatyczne wykrywanie aktywów 4. automatyczne wykrywanie podatności 5. automatyczne wykrywanie anomalii 6. automatyczne grupowanie aktywów 7. predefiniowane reguły analizy i korelacji zdarzeń 8. łatwe w użyciu mechanizmy filtrowania (również predefiniowane filtry) 9. zaawansowane funkcje analizy zabezpieczeń 10. predefiniowane raporty 11. priorytetyzacja wg zasobów 12. automatyczne aktualizacje baz zagrożeń, wsparcia urządzeń, oprogramowania systemowego, |
| Rozwiązanie musi udostępniać graficzny interfejs webowy do zarządzania, analizy i raportowania. Zalecanym jest, aby interfejs nie wymagał żadnych wtyczek typu Java, Flash lub wymogu posiadania grubego klienta do obsługi rozwiązania. |
| Rozwiązanie musi posiadać własne i/lub wspierać zewnętrzne mechanizmy HA, szczególnie w zakresie mechanizmów akwizycji i przechowywania danych oraz centralnego zarządzania systemem. |
| Rozwiązanie musi zapewniać ciągłe działanie jak największej liczby komponentów, niezależnie od awarii jednego z nich. Np. w sytuacji awarii systemu centralnego lub modułu analitycznego, logi powinny być nadal zbierane. |
| Rozwiązanie musi posiadać mechanizmy umożliwiające zbieranie danych w czasie rzeczywistym. Nadto rozwiązanie powinno posiadać możliwość zbierania i buforowania danych w lokalnym kolektorze na czas gdy centralne repozytorium nie jest dostępne, zaś po udostępnieniu centralnego repozytorium natychmiastowego wysłania zbuforowanych danych. |
| Rozwiązanie musi posiadać zautomatyzowany proces wykonywania backupu i odzyskiwania konfiguracji z backupu. |
| Rozwiązanie musi posiadać automatyczny mechanizm kontroli stanu swoich komponentów (health check), wraz z informowaniem użytkownika o zauważonych problemach. |
| Rozwiązanie powinno posiadać przykładowe skonfigurowanych panele (dashboards), prezentujące możliwości i mechanizmy systemu SIEM. |
| Rozwiązanie musi utrzymywać bazę wiedzy o wszystkich wykrytych w sieci aktywach. Baza danych o aktywach powinna umożliwiać edycję zebranych informacji, zapewniając jednak ochronę przed nieuprawnioną zmianą, oraz rozliczalność procesu wprowadzania zmian. Baza danych musi umożliwiać przeszukiwanie swojej zawartości. Wśród zgromadzonych danych o danym aktywie powinny być zawarte pewne informacje uzyskane przy wykrywaniu zasobów:   1. atrybuty systemu 2. atrybuty sieciowe 3. stan 4. podatności/luki 5. lokalizacja 6. przynależność 7. inne właściwości, które użytkownik może samodzielnie zdefiniować i/lub wpisywać |
| Rozwiązanie musi być zdolne obsłużyć nagły wzrost liczby zbieranych danych (EPS) jednocześnie zapewniając, ciągłość zbierania danych, tak aby żaden przepływ sieciowy lub żadne zdarzenie nie zostało pominięte. W takiej sytuacji system musi jednocześnie zachować pełna funkcjonalność. |
| Rozwiązanie musi wspierać/obsługiwać produkty innych producentów w zakresie bezpieczeństwa. |
| Rozwiązanie musi wspierać informacje zbierane z systemów operacyjnych firmy Microsoft, zarówno wersji serwerowych, aplikacyjnych i funkcjonalnych, jak również z systemów użytkowników końcowych. |
| Rozwiązanie musi wspierać informacje zebrane z systemów opartych na środowiskach firmy Microsoft, w szczególności:   1. Microsoft Sharepoint Server 2. Microsoft Exchange Server 3. Microsoft IIS 4. Microsoft AD 5. Microsoft FS 6. Inne |
| Rozwiązanie musi wspierać informacje zbierane z systemów komercyjnych (np. serwery WWW/FTP, systemy ERP, SAP, itp.). |
| Rozwiązanie musi wspierać informacje zebrane z systemów i narzędzi zabezpieczających klasy DLP (Data Leak Protection). |
| System musi umożliwiać realizację wsparcia dla danych zbieranych z systemów wytworzonych w ramach prac własnych i innych niestandardowych, realizowanych w ramach zamówień indywidualnych. Aby zrealizować takie wymaganie producent i system musi umożliwiać użytkownikowi końcowemu samodzielne i nieodpłatne (bez dodatkowych licencji i kosztów w tym wsparcia technicznego), budować własne parsery logów. |
| Rozwiązanie musi wspierać informacje zebrane z systemów zabezpieczeń klasy DAM (Database Activity Monitoring). |
| Możliwość wykorzystania informacji dotyczących plików - zebranych z systemów i narzędzi bezpieczeństwa klasy FIM/FAM (File Integrity/Activity Monitoring) lub poprzez rozwiązania agentowe. |
| Rozwiązanie musi wspierać informacje zebrane z systemów i narzędzi bezpieczeństwa klasy IAM (Identity and Access Management). |
| Rozwiązanie musi wspierać informacje typu: użytkownicy, grupy, zebrane z usługi katalogowej (np. AD, LDAP), poprzez interfejs integracyjny lub plik. |
| Rozwiązanie musi wspierać informacje NetFlow - czyli dane o przepływach, np.: NetFlow, J- Flow, sFlow, itp., zebrane samodzielnie jak również za pomocą innych narzędzi. |
| Rozwiązanie musi wspierać informacje zebrane z infrastruktury sieciowej (switche, routery, itp.). |
| Rozwiązanie musi wspierać informacje zebrane z wiodących skanerów podatności. |
| Rozwiązanie musi posiadać architekturę pozwalającą na zbieranie i archiwizację logów, w podziale na dane krótkoterminowe (tzw. online, wykorzystywane w bieżących analizach) oraz dane długoterminowe (tzw. offline, dane archiwizowane po określnym czasie), z wewnętrzną ale konfigurowalną obsługą mechanizmu retencji danych pomiędzy obydwoma typami. |
| Zamawiający oczekuje przechowywania logów przez okres minimum 24 miesięcy, gdzie minimum 6 miesięcy to dostęp online dla celów analitycznych. Ponadto zamawiający oczekuje możliwości zapisu i kompresji/archiwizacji danych, przy wykorzystaniu konfigurowalnych mechanizmów retencji, wbudowanych w system, do 5 lat wstecz. |
| Rozwiązanie powinno wspierać przechowywanie (archiwizację) logów na zewnętrznych (3rd party) urządzeniach do składowania danych. |
| Rozwiązanie musi posiadać mechanizmy umożliwiające na efektywne przechowywanie i kompresję zbieranych danych. |
| Rozwiązanie musi wspierać branżowe mechanizmy zbierania logów (np.: syslog, WMI, JDBC, SNMP, Checkpoint, itp.). |
| Rozwiązanie musi wspierać bez-agentowe zbieranie danych, w miarę możliwości w jak największej liczbie przypadków. |
| System powinien wspierać analizę logów z sytemu MS Windows. |
| Rozwiązanie musi wspierać długoterminowe zapewnienie dostępu do szczegółowych danych odnośnie zarejestrowanych i zebranych zdarzeń czy przepływów w sieci. System powinien zapewnić dostęp do takich informacje co najmniej przez okres 12 miesięcy (Zamawiający oczekuje przechowywania surowych danych sieciowych przez okres minimum 3 miesięcy, zaś dla danych typu flow, minimum 12 miesięcy). |
| Rozwiązanie musi normalizować informacje zawarte w zebranych zdarzeniach (usernames, IP address, hostnames, log source, device, itp.), z urządzeń i systemów różnych dostawców. |
| Rozwiązanie musi wspierać mechanizm jednolitej i wspólnej taksonomii/klasyfikacji zdarzeń. |
| Rozwiązanie musi zapewniać możliwość przechowywania zarówno znormalizowanych danych o zdarzeniach, jak również źródłowego/oryginalnego formatu danych w tzw. postaci RAW (fuli payload indexing), np. dl celów późniejszej analizy w innych systemach lub przeprowadzenia analizy śledczej. |
| Rozwiązanie musi umożliwiać normalizację i agregację pól w zdarzeniach, które nie są dostępne domyślnie w istniejących mechanizmach normalizacji. |
| Rozwiązanie musi obsługiwać i/lub normalizować sygnatury czasowe zdarzeń w wielu strefach czasowych, |
| Rozwiązanie musi zapewniać analizę w czasie rzeczywistym. |
| Rozwiązanie musi zapewnić długoterminową analizę zdarzeń w poszukiwaniu tendencji incydentów. |
| Rozwiązanie musi zapewnić możliwość agregowania i analizowania zdarzeń opartych na filtrze określonego użytkownika. |
| Rozwiązanie musi umożliwiać prezentację zdarzeń w trybie real-time, przy jednoczesnym zapewnieniu pełnej funkcjonalności filtrowania prezentowanych zdarzeń. |
| Rozwiązanie musi zapewnić mechanizmy alarmowania w oparciu o zaobserwowane nieprawidłowości i zmian behawioralnych w zdarzeniach sieciowych i zdarzeniach dotyczących bezpieczeństwa. |
| Rozwiązanie musi zapewniać tworzenie i utrzymywanie historii aktywności użytkowników systemu na poszczególnych zasobach zarejestrowanych w systemie (korelacja users per assets) |
| Rozwiązanie musi zapewniać raportowanie dla wszystkich przedmiotów dostępnych poprzez GUI systemu (np.: pobrane dane, zanalizowane dane, zdarzenia, przepływy, podatności, zasoby, zagrożenia, itp.). |
| Rozwiązanie powinno w standardzie (out-of-the-box) zawierać zestaw gotowych raportów, obejmujących kategorie: uwierzytelnianie, tożsamość, aktywność użytkowników, zgodność, konfiguracja i zarządzanie zmianą, raport zarządczy, raporty dotyczące urządzeń, zarządzanie siecią, bezpieczeństwo, monitorowanie użycia, aktywność aplikacji. |
| Rozwiązanie musi wspierać mechanizm priorytetyzacji (wagi) zgłaszanych alarmów i komunikatów, powstałych na podstawie wykonanej analizy i wagi zdarzeń oraz wartości zasobu. Wymaganym jest aby waga alertu zależała od kilku zmiennych, np.: rodzaj zasobu, zasób, protokół, aplikacja, reguła korelacyjna, źródło zdarzenia (kolektor/skaner podatności/analityka SIEM), itp. Ustawienie tej wagi musi być możliwe bez dodatkowych kosztów i wsparcia technicznego ze strony producenta. |
| Rozwiązanie musi posiadać zdolność monitorowania dzienników zdarzeń pod kątem anomalii, awarii, zmian w pobranych danych. W przypadku wykrycia niezgodności lub błędu w działaniu logu lub pobieraniu zdarzeń z logu, rozwiązanie powinno wygenerować alert. |
| Rozwiązanie powinno w standardzie (out-of-the-box) zapewniać mechanizmy zdolne do wykrywania i klasyfikacji zasobów wg typu systemu, rozpoznając np.: systemy pocztowe, serwery plików, serwery bazodanowe, itp. |
| Rozwiązanie musi posiadać zdolność do wykrywania ataków typu DoS (Denial of Service) oraz DDoS (Distributed Denial of Service). |
| Licencje powinny być bezterminowe i nie uzależnione od wykupienia lub przedłużenia wsparcia producenta. |
| Dostawca gwarantuje, że rozwiązanie będzie wspierane przez co najmniej 5 lat, i w tym czasie nie nastąpi wstrzymanie wsparcia dla zakupionego produktu (EoL – End of Life, EoS – End of Support). |
| Mechanizm analizy przebiegu incydentu powinien wykorzystywać zgromadzone dane, uwzględniające zdarzenia w logach, przepływy netflow, a także pełne zrzuty danych pakietowych oraz dane zgromadzone w plikach. System powinien umożliwiać analizy danych dostępnych na Twitterze, Facebooku, wynikach wyszukiwania, dokumentach wytwarzanych przez aplikacje, pakietach VoIP (w tym możliwość odtworzenia konwersacji). |
| Możliwość analizy na poziomie sieciowym, kto był zaangażowany w incydent, co się stało, kiedy zaszło zdarzenie, jakie dane zostały udostępnione lub przekazane. |
| Możliwość wyszukiwania malware'u i aktywności związanych z jego działaniem. |

1. **System monitorowania usługi Liczba sztuk: 1**

**Oferowane oprogramowanie\* ……………………..\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Monitorowanie dostępności usług i aplikacji, co najmniej:   1. poczty email: SMTP, POP3 2. usług www: HTTP, HTTPS 3. usług i aplikacji WEB za pomocą: SOAP 4. usług DNS za pomocą protokołu DNS 5. usług i aplikacji za pomocą specyficznych portów TCP |
| Monitorowanie statusu i wydajności krytycznych aplikacji biznesowych, w tym co najmniej: systemów Microsoft Windows (procesów, usług i zdarzeń), Microsoft Active Directory (LDAP), serwerów pocztowych (SMTP, POP3), serwerów WWW, usług DNS, serwerów Linux |
| Monitorowanie usług typu LDAP, WEB, RADIUS przez specjalnie do tego celu skonfigurowanego użytkownika |
| System umożliwia odwzorowanie struktury logicznej monitorowanych zasobów, usług i aplikacji oraz umożliwia odwzorowanie struktury działania aplikacji tj. zależności pomiędzy warstwami prezentacji, aplikacji i bazy danych |
| System może pracować zarówno w konfiguracji wymagającej instalacji agenta programowego na monitorowanym zasobie, jak i w konfiguracji bez agentowej |
| System umożliwia wyświetlanie dla monitorowanych aplikacji i usług informacji o: czasie odpowiedzi, obciążeniu procesora, wykorzystaniu pamięci (fizycznej i wirtualnej) |
| System udostępnia administratorom informacje o monitorowanych zasobach w podręcznym menu: status aplikacji, status serwera, obciążenie procesora, wykorzystanie pamięci |
| System umożliwia elastyczne definiowanie reguł monitorowania dostępności usług, zasobów i aplikacji |
| System umożliwia definiowanie i dodawania własnych dodatków rozszerzających możliwości monitoringu , w tym wspiera następujące języki programowania dla dodatków rozszerzających możliwości monitoringu: C, Python, Perl, Java |
| System udostępnia interfejs www umożliwiający podgląd stanu monitorowanych aplikacji i usług. System posiada możliwość personalizacji interfejsu aplikacji, administratorzy muszą mieć możliwość edytowania wyglądu i dostosowania interfejsu do własnych potrzeb |
| System umożliwia powiadamianie administratora o zdarzeniach (alarmy i awarie) przez email lub SMS oraz zapewnienia reakcję na awarie (np. wysłanie wiadomości e-mail, SMS, wykonanie skryptu, itp.) |
| System umożliwia zbieranie i wyświetlanie statystyk dostępności |
| System dysponuje mechanizmami raportowania umożliwiającymi elastyczne konfigurowanie raportów dotyczących dostępności monitorowanych usług i zasobów |
| System posiada możliwość konfiguracji kont użytkowników oraz przypisywanie im uprawnień tylko do odpowiednich raportów |
| System posiada możliwość konfiguracji bazy administratorów wraz z ich uprawnieniami tzn.:   1. konfigurację kont administratorów posiadających możliwość monitorowania wszystkich zasobów 2. konfigurację kont operatorów posiadających możliwość monitorowania wszystkich zasobów w danej grupie (lokalizacji) 3. konfigurację kont posiadających uprawnienia jedynie do wyświetlenia stanu wybranych zasobów (view only, read only) bez możliwości edycji i zmiany uprawnień i konfiguracji |

1. **Szafa RACK wyposażona w listwy PDU Liczba sztuk: 6**

**Oferowany model \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Szafa o wysokości 42U szerokości 800mm, głębokości 1000mm. |
| Szafy wyposażone w system dystrybucji zasilania w postaci inteligentnych listew zasilających |
| Rama szafy spawana z zamkniętego profilu, wyposażonego w liczne otwory na nakrętki koszykowe oraz wkręty samoformujące. |
| Osłony boczne zamykane na kluczyk. |
| Drzwi przednie i tylne jednoskrzydłowe, płaskie, perforowane z optymalizowaną powierzchnią perforacji 80% dla wydajniejszego chłodzenia. Drzwi z zawiasami, wyposażone w zamek. |
| Płaszczyzna montażowa składająca się z 4 galwanizowanych, numerowanych profili, każda z zaznaczona wysokością U. Łączna obciążalność statyczna płaszczyzny montażowej nie może wynosić mniej niż 800 kg. |
| Dach szafy modułowy z możliwością demontażu, wyposażony w otwory umożliwiające montaż przepustów kablowych. |
| Wejścia okablowania strukturalnego zabezpieczone przepustem (np. szczotkowym). |
| Szafa wyposażona w dwie galwanizowane, pionowe drabinki kablowe na całą wysokość szafy mocowane do ramy szafy do prowadzenie okablowania . |
| Szafa musi posiadać pionowe panele zapewniające odpowiednią separacje frontów szaf i chroniące przed mieszaniem powietrza przód - tył |
| Puste przestrzenie montażowe zaślepione odpowiednią ilością zaślepek 1U lub 2U montowanych bez narzędziowo np. za pomocą plastikowych spinek. |
| Na każdy zainstalowany panel światłowodowy należy zamontować szufladę zapasu kabla, |
| Szafa musi być posadowiona na cokole min. 100mm |
| Szafa musi umożliwiać montaż min. dwóch pionowych listw PDU do ramy szafy. |
| Wyposażenie w panele ułatwiające organizację kabli połączeniowych musi obejmować każde 24 porty okablowania miedzianego lub światłowodowego. |
| Konstrukcja zabudowy spawana. |
| Przyłączeniowa listwa uziemiająca z blachy miedzianej. |
| |  | | --- | | Zgodność z normami EIA-310 | | Zgodność z normami RoHS | |
| Każda listwa ma być wyposażona w minimum 36 gniazd IEC320 C13 oraz 6 gniazda IEC320 C19. Obudowa listwy nie może przekraczać na szerokość 67 mm i na głębokość 45 mm. Listwa montowana do ramy szafy, z boku w taki sposób aby kable zasilające wpięte do listwy nie nachodziły na przednią i tylną przestrzeń montażową szafy |

1. **Oprogramowanie typu skaner podatności- narzędzie do wsparcia testów bezpieczeństwa aplikacji WEB**

**Oferowane oprogramowanie \* ……………………..\* Producent \* …………………..**

**Sposób licencjonowania: ……………………………………………** *(proszę wskazać sposób licencjonowania produktu np. na rdzeń procesora, na procesor itp.)*

**Ilość dostarczanych licencji: ………………………………………….**

| **Opis wymagań minimalnych** |
| --- |
| Narzędzie musi udostępniać jednorodne i spójne środowisko pracy testera |
| Narzędzie musi pozwalać na pracę w środowisku systemów MS Windows, macOS i Linux. |
| Narzędzie musi pozwalać na analizowanie kodu aplikacji pod kontem występowania podatności, w tym podatności występujących na listach OWASP TOP10 i CWE TOP25 |
| Narzędzie musi wspierać fazę zbierania informacji, w zakresie weryfikacji charakteru żądań i odpowiedzi HTTP/HTTPS oraz analizy struktury aplikacji |
| Narzędzie musi wspierać analizę punktów wejścia aplikacji |
| Narzędzie musi wspierać tworzenie próbek aplikacji, "fuzzowanie" parametrów aplikacji i automatyczne znajdowania błędów aplikacji |
| Narzędzie musi posiadać funkcjonalność lokalnego serwera proxy pozwalającą na kontrolę i analizę ruchy HTTP/HTTPS przesyłanego pomiędzy przeglądarką testera a serwerem WWW testowanej aplikacji |
| * Narzędzie musi umożliwiać budowę i analizę drzewa badanej strony, oraz definiowanie zasięgu testów. |
| Narzędzie musi posiadać możliwość nagrywania i analizy ruchu (wysłanych zapytań i odpowiedzi aplikacji), zbierania próbki standardowej funkcjonalności aplikacji i tworzenia nowych zapytań na podstawie wcześniej zebranej próbki |
| Narzędzie musi posiadań możliwość nagrywania sesji testowych, oraz modyfikacji i odtwarzania sesji testowych |
| Narzędzie musi posiadań wsparcie dla automatycznej enumeracji zasobów, wysyłania żądań, oraz wspierać ocenę praktycznej entropii losowych wartości, w tym dla np. ciasteczek, tokenów, identyfikatorów obiektów. |
| Narzędzie musi posiadać wbudowaną funkcjonalność raportową pozwalającą na generowanie raportów z przeprowadzonych testów bezpieczeństwa |

1. **Oprogramowanie typu monitor podatności Liczba sztuk: 1**

**Oferowane oprogramowanie \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Skanowanie systemów operacyjnych serwerów, serwerów WWW i urządzeń sieciowych w poszukiwaniu typowych błędów konfiguracji zabezpieczeń; |
| Skanowanie systemów operacyjnych serwerów, serwerów WWW i urządzeń sieciowych pod kątem wystąpienia luk stanowiących ryzyko dla bezpieczeństwa; |
| Skanowanie systemów pod kątem aktualności zainstalowanych uzupełnień; |
| Wykrywanie kont lokalnych niezgodnych z aktualną polityką bezpieczeństwa (np. posiadających puste hasła); |
| Weryfikacja zgodności aktualnych zabezpieczeń z bieżącymi zaleceniami i politykami bezpieczeństwa. |
| Musi posiadać możliwość regularnej aktualizacji zarówno samego oprogramowania jak i bazy podatności przez okres co najmniej 36 miesięcy od dnia obioru przedmiotu umowy |

1. **Oprogramowanie do zarządzania siecią Liczba sztuk: 1**

**Oferowane oprogramowanie \* ……………………..\*\* Producent \* …………………..**

| **Opis wymagań minimalnych** |
| --- |
| Oprogramowania do zarządzania siecią przewodową musi umożliwiać zarządzanie siecią składającą się z przełączników LAN ( Typ 1, Typ 2 Typ3) |
| Oprogramowanie musi być zbudowane w architekturze klient – serwer. |
| Oprogramowanie musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) |
| Oprogramowanie musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników lub zewnętrznych systemów LDAP, z wymuszeniem reguł złożoności haseł dla administratorów |
| Oprogramowanie musi pozwalać na hierarchizację zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów i zewnętrznego serwera uwierzytelniającego. Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń |
| Licencja na system powinna umożliwiać zarządzanie minimum 100 urządzeniami sieciowymi różnych producentów z możliwością rozbudowy do przynajmniej 5000 urządzeń sieciowych |
| Oprogramowanie musi minimalnie wspierać instalację części serwerowej na platformach Windows Server 2012 R2, Windows Server 2016 lub Red Hat Enterprise Linux 6.x. |
| Oprogramowanie musi być zbudowane modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność. |
| Oprogramowanie do zarządzania musi spełniać podstawowe funkcje:   1. automatyczną identyfikację i wyszukiwanie urządzeń instalowanych w sieci. Możliwość ręcznego i automatycznego dodawania urządzeń 2. automatyczne wykrywanie topologii sieci z użyciem minimum protokołów SNMP, Telnet lub innych mechanizmów 3. monitorowanie stanu urządzeń 4. konfigurację urządzeń 5. konfigurację list dostępu (ACL) na zarządzanych urządzeniach 6. konfigurację VLANów na zarządzanych urządzeniach 7. zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania 8. funkcje przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń 9. narzędzie do zarządzania obrazami oprogramowania urządzeń 10. zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń 11. możliwość wysyłania alarmów np. mailem lub SMS’em 12. generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta 13. prezentację urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu każdego urządzenia 14. obrazowanie sieci w postaci hierarchicznych map (urządzania wraz z połączeniami fizycznymi i logicznymi) wraz z wizualizacją alarmów oraz wizualizacją poszczególnych szaf telekomunikacyjnych 15. podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy 16. wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych 17. tworzenie wzorców i szablonów konfiguracji na urządzenia 18. funkcję Telnet / SSH proxy umożliwiającą zarządzanie CLI przez przeglądarkę Internetową. 19. funkcję zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android. 20. dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową. 21. niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z LDAP / Active Directory minimum w zakresie pobierania grup, kont administratorów 22. zbieranie informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, Email lub exportu do plików csv/pdf 23. kontekstową funkcje pomocy zmieniającą zawartość w zależności od wyświetlanego kontekstu. |