|  |  |  |
| --- | --- | --- |
|  |  | |
| Strona |  |
| z ogólnej liczby |  |

*(pieczęć Wykonawcy)*

ZAŁĄCZNIK Nr 4

ZESTAWIENIE PARAMETRÓW OFEROWANEGO SPRZĘTU INNEGO NIŻ WYMIENIONY W SIWZ, PARAMETRY TE BĘDĄ OCENIANE JAKO RÓWNOWAŻNE

Uwaga: wypełnia wyłączenie Wykonawca oferujący sprzęt o parametrach innych niż wymienione w SIWZ. Różnice należy wpisać drukowanymi literami tylko w wierszach, w których zapisy SIWZ są różne. Jeżeli oferowane sprzęt i oprogramowanie jest zgodne z zapisami SIWZ wówczas nie należy wypełniać tego załącznika

1***.*Komputer przenośmy (laptop) - 3 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp | Parametr | Wymagane minimalne parametry techniczne | Parametry oferowane |
| 1 | Procesor | dwurdzeniowy |  |
| 2 | Dysk Twardy | 320 GB |  |
| 3 | Zainstalowana pamięć RAM | 2 GB |  |
| 4 | Przekątna ekranu | 15 ‘’ |  |
| 5 | Napęd wbudowany | DVD/RW |  |
| 6 | Złącza zewnętrzne | VGA  3 x USB  czytnik kart  1 x RJ45 |  |
| 7 | System operacyjny | Microsoft Windows 7 lub Windows 8.1 z możliwością downgrade |  |
| 8 | Program antywirusowy | ESET NOD 32 Endpoint  **Licencja – 2 lata (min. =max)** |  |
| 9 | Gwarancja | 2 lata |  |

2. Router sieciowy - 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Parametr | Wymagane minimalne parametry techniczne | Parametry oferowane |
| 1. | Porty | 12 portów 10/100/1000 |  |
| 2. | Zapora korporacyjna (firewall) | Urządzenie ma obsługiwać translacje adresów NAT, PAT, 1-PAT  Urządzenie ma dawać możliwość ustawienia trybu pracy jako router, bridge lub hybrydowo (część jako router a część jako bridge)  Administrator ma możliwość zdefiniowania minimum 10 różnych zestawów reguł  Edytor reguł na firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wykazuje na użycie nieistniejących elementów sieciowych (obiektów)  Firewall ma możliwość uwierzytelniania i autoryzację użytkowników w oparciu o bazę lokalną lub zewnętrzny serwer |  |
| 3. | Intrusion Prevention System (IPS) | IPS ma być zaimplementowane w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów oraz analizy heurystycznej  Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.  Moduł IPS ma zabezpieczać co najmniej 10000 ataków i zagrożeń  Moduł IPS ma nie tylko wykrywać ale i usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. |  |
| 4. | Kształtowanie pasma | Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytezację ruchu oraz minimalną i maksymalną wartość pasma.  Ograniczanie pasma ma być określane względem reguły na firewallu w odniesieniu do adresu IP, autoryzowanego użytkownika  Rozwiązanie ma umożliwiać tworzenie tzw. Kolejki nie mającej wpływu na kształtowanie pasma a na śledzenie konkretnego typu ruchu (monitoring) |  |
| 5. | Ochrona antywirusowa | Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych w tym jednego dostarczonego przez firmy trzecie (inny niż producent rozwiązania).  Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej i bezpłatnej licencji.  Administrator ma mieć możliwość definiowania maksymalnego pliku do skanowania programem antywirusowym.  Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. |  |
| 6. | Ochrona ANTYSPAM | Urządzenie ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest poczta niechcianą (SPAM)  Ochrona antyspam ma działać w oparciu o:   1. Białe/czarne listy 2. DNS RBL, 3. Heurystyczny skaner   W przypadku ochrony o DNS RBL administrator może modyfikować listę serwerów RBL |  |
| 7. | Wirtualne sieci prywatne (VPN) | Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-side (klient mobilny – lokalizacja) lub site-to-site (lokalizacja –lokalizacja).  Kanały VPN można budować o: - PPTP VPN - IPSec VPN - SSL VPN |  |
| 8. | Filtr adresów URL | Urządzenie ma posiadać wbudowany filtr URL.  Filtr URL ma działać w oparciu o klasyfikację URL dostarczaną przez producenta zawierającą co najmniej 50 kategorii tematycznych stron internetowych.  Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.  Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech opcji: - blokowanie dostępu do adresu URL, - zezwolenie na dostęp do adresu URL, - blokowanie dostępu do adresu URL, z jednoczesnym wyświetleniem komunikatu  Filtrowanie musi uwzględniać także komunikację po protokole HTTPS |  |
| 9. | Uwierzytelnianie | Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:  - lokalną bazę użytkowników (wewnętrzny LDAP) - zewnętrzną bazę użytkowników (zewnętrzny LDAP) - integrację z serwerem Microsoft Active Directory.  Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły : ssl, Radius, Kerberos. |  |
| 10. | Administracja łączami od dostawców usług internetowych (ISP) | Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia do sieci Internet (tzw. Load Balancing)  Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |  |
| 11. | Pozostałe usługi i funkcje | Urządzenie posiada wbudowany serwer DHCP z możliwością przypisania adresu IP do adresu MAC karty sieciowej  Urządzenie musi umożliwiać przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay  Urządzenie musi posiadać usługę klienta NTP. |  |
| 12. | Administracja urządzeniem | Urządzenie ma posiadać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.  Konfiguracja urządzenia musi być dostępna z wykorzystaniem polskiego interfejsu graficznego  Interfejs konfiguracyjny musi być dostępny przez przeglądarkę internetową a komunikacja ma być zabezpieczona protokołem https.  Komunikacja może odbywać na porcie innym niż 443 TCP.  Urządzenie może być zarządzane przez dowolną liczbę administratorów.  Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). |  |
| 13. | Raportowanie | Urządzenie ma być dostarczone wraz z dedykowanym systemem raportowania, oparte o darmowy system np. Linux.  Interfejs użytkownika musi być dostępny przez przeglądarkę internetową.  Interfejs użytkownika narzędzia raportującego ma być dostępny w dwóch językach – polskim i angielskim.  Przesyłanie logów pomiędzy urządzeniem a narzędziem raportującym musi odbywać się za pomocą protokołu syslog.  Rozwiązanie musi posiadać możliwość wygenerowania raportów graficznych na podstawie zebranych logów, w tym co najmniej:   1. Raporty WEBzawierające informacje o: odwiedzanych stronach WWW, ilości połączeń do tych stron, ilość pobranych danych, kategoriach tematycznych, do których należą te strony, użytkownikach, którzy łączyli się z danymi adresami oraz adresach IP z których wychodzono na owe strony 2. Raporty skanera sieci zawierające informacje o: wykrytych zagrożeniach w aplikacjach 3. Raporty IPS zawierające wykryte zagrożenia oraz adresy docelowe i źródłowe których te zagrożenia dotyczą   Raporty graficzne muszą oferować możliwość:  - przeszukiwania zgromadzonych informacji, - wyświetlenia zgromadzonych informacji dla wybranego dnia, tygodnia, miesiąca, - eksportu do zewnętrznych plików obsługujących format PDF lub CSV  Narzędzie raportujące musi być dostarczane w ramach podstawowej licencji bez dodatkowych opłat. |  |
| 14. | Parametry sprzętowe | Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 120 GB do tzw. Raportowania.  Liczba portów Ethernet 10/100/1000 min. 12  Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.  Urządzenie pozwala na użycie 8 niezależnych łączy WAN.  Minimalna przepustowość Firewalla wraz z włączonym systemem IPS – 1 500 Mbps Minimalna przepustowość tunelu VPN prze szyfrowaniu AES wynosi min. 350 Mbps  Liczba tuneli VPN Ipsec nie może być mniejsza niż 1000  Obsługa min. 512 VLAN  MAX liczba równoczesnych sesji nie mniej jak 600 000  Urządzenie nie jest limitowane na użytkowników. |  |
| 15. | Serwis | Serwis i wsparcie techniczne na min. 1 rok |  |

3. Dysk sieciowy - 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| Lp | Parametr | Wymagane minimalne parametry techniczne | Parametry oferowane |
| 1 | Ilość zainstalowanych dysków | 2 szt. |  |
| 2 | Pojemność | 2 x 1 TB (3,5” SATA) |  |
| 3 | Interfejsy | 1xRJ45 1xUSB 2.0 |  |
| 4 | Gwarancja | 2 lata |  |

Upełnomocniony przedstawiciel

.................................................

*(podpis, pieczęć)*

Data : ................................................