Opis wymaganych funkcjonalności urządzeń

1. **Zapora – urządzenie centralne, siedziba główna – Przemysłowa 17**
2. Wbudowane mechanizmy ochrony sieci
3. Obsługa ochrony poczty e-mail – scentralizowana obsługa usługi Microsoft 365 na urządzeniu wraz z opcją dostosowywania reguł filtracji mailów, oraz obsługa czarnej/białej listy oraz obsługa wykluczeń i wyjątków
4. Możliwość zapisania lokalnie maila/załącznika zakwalifikowanego jako podejrzany/zagrożony
5. Wbudowane mechanizmy wykrywania zagrożeń oraz ochrony przed nimi
6. Wbudowane mechanizmy zapobiegające włamaniom i atakom (DoS, DDos, skanowanie portów)
7. Obsługa wielu łącz internetowych z możliwością load-balacingu oraz opcją automatycznego przełączania w przypadku awarii łącza
8. Realizacja połączeń VPN w różnych dostępnych technologiach - IP-Sec, SSL VPN, L2TP, PPTP, Site-to-site VPN
9. Wbudowane mechanizmy automatycznego przełączania połączenia VPN w przypadku braku dostępności łącza po stronie KM-Płock (failover group)
10. Obsługa minimum 2 połączeń z APN (Orange, Plus) wraz z łączami zapasowymi po stronie KM-Płock
11. Obsługa tunelów gre
12. Obsługa dedykowanych tunelów z Microsoft Azure
13. Dostęp do urządzenia przez SSH, https, dedykowany portal
14. Obsługa dostępu klientów VPN z podziałem na uprawnienia wraz z obsługą z urządzeń z systemami Windows/MacOS/Android/Linux
15. Dostęp pracowników przez dedykowanego klienta dla realizacji Okazjonalnej Pracy Zdalnej z autoryzacją na poziomie użytkownika i możliwością zmiany hasła tylko po udanej autoryzacji
16. Możliwość tworzenia grup użytkowników, użytkowników oraz przypisywania im ról
17. Możliwość konfiguracji routingów (static, OSPF, BGP, multicast)
18. Tworzenie reguł firewalla dla określonych połączeń/typów połączeń VPN/LAN/WAN/DMZ
19. Tworzenie reguł NAT oraz przekierowywań
20. Inspekcja ruchu SSL/TSL
21. Ochrona przed atakami Zero-day
22. Śledzenie połączeń: FTP, IRC, PPTP, TFTP
23. Obsługa DHCP
24. Wbudowany antywirus oraz antymalware wraz z opcją zewnętrznego silnika sprawdzającego
25. Rozbudowany moduł raportowania obsługujący m.in. raportowanie ruchu sieciowego z/do danego hosta, ilość wywołań z/do danego hosta, połączenia odrzucone, połączenia zaakceptowane wraz z możliwością eksportu raportów do plików .csv/.txt
26. Wysyłanie na maila i SMS informacji o zaistniałych zagrożeniach/zdarzeniach
27. Panel aktualnego: stanu urządzenia, aktywnych połączeń VPN, połączeń klientów zdalnych, połączeń do urządzenia
28. Funkcje diagnostyczne
29. Blokowanie i ochrona stron www – możliwość tworzenia polis dostępowych/kategorii wraz z dostosowywaniem akcji (blokowanie, ostrzeżenie, informacja), obsługa białej/czarnej listy, obsługa wyjątków oraz wyłączeń, obsługa blokowania plików o określonych rozszerzeniach
30. Automatyczna aktualizacja listy blokowanych stron pobierana z pliku .txt z zewnętrznego hosta (http://hole.cert.pl/domains/domains.txt)
31. Obsługa web proxy, SNMP, SMTP Relay
32. Kontrola aplikacji – możliwość monitorowania używania aplikacji
33. Automatyczne tworzenie kopii konfiguracji zabezpieczonej hasłem na zasobie zewnętrznym
34. Możliwość tworzenia profilów: harmonogramów, godzin dostępów, limitów użytkowania internetu, limitów danych, odszyfrowywania, połączeń IPSec, dostępów do urządzenia)
35. Możliwość tworzenia list: hostów IP, grup hostów IP, hostów MAC, hostów FQDN, grup hostów FQDN, grup lokalizacyjnych, usług, grup usług)
36. Możliwość tworzenia list ACL (dla użytkowników/ grup/ połączeń VPN)
37. Możliwość ręcznego ustawienia portu dostępowego do urządzenia oraz portu dostępu do portalu użytkownika
38. Możliwość ustawienia kontroli złożoności hasła dostępowego do urządzenia dla różnych grup użytkowników
39. Automatyczna aktualizacja bibliotek urządzania wraz z możliwością zarządzania wersją firmware’u urządzania
40. Blokowanie wysyłania informacji poufnych w tle z już zainfekowanych komputerów
41. Zamawiający aktualnie posiada rozwiązanie bazujące na 2 urządzeniach, głównym oraz zapasowym. Kopia konfiguracji urządzenia głównego jest wykonywana automatycznie raz dziennie na zasób sieciowy. W przypadku awarii urządzenia głównego następuje ręczne przeniesienie ostatniej konfiguracji na urządzenie zapasowe a następnie przełączenie na urządzenie zapasowe poprzez przepięcie kabli sieciowych. Zamawiający dopuszcza inne niż opisane rozwiązanie, zapewniające zachowanie ciągłości pracy w przypadku awarii urządzenia centralnego.
42. **Zapora – urządzenia na lokalizacjach wyniesionych – 2 lokalizacje: Jachowicza 42, Kolegialna 3**
43. Wbudowane mechanizmy ochrony sieci
44. Wbudowane mechanizmy wykrywania zagrożeń oraz ochrony przed nimi
45. Wbudowane mechanizmy zapobiegające włamaniom i atakom (DoS, DDos, skanowanie portów)
46. Obsługa wielu łącz internetowych z możliwością load-balacingu oraz opcją automatycznego przełączania w przypadku awarii łącza
47. Realizacja połączeń VPN w różnych dostępnych technologiach - IP-Sec, SSL VPN, L2TP, PPTP, Site-to-site VPN
48. Wbudowane mechanizmy automatycznego przełączania połączenia VPN w przypadku braku dostępności łącza po stronie KM-Płock (failover group)
49. Obsługa dedykowanych tunelów z Microsoft Azure
50. Dostęp do urządzenia przez SSH, https, dedykowany portal
51. Obsługa dostępu klientów VPN z podziałem na uprawnienia wraz z obsługą z urządzeń z systemami Windows/MacOS/Android/Linux
52. Możliwość tworzenia grup użytkowników, użytkowników oraz przypisywania im ról
53. Możliwość konfiguracji routingów (static, OSPF, BGP, multicast)
54. Tworzenie reguł firewalla dla określonych połączeń/typów połączeń VPN/LAN/WAN/DMZ
55. Tworzenie reguł NAT oraz przekierowywań
56. Inspekcja ruchu SSL/TSL
57. Ochrona przed atakami Zero-day
58. Śledzenie połączeń: FTP, IRC, PPTP, TFTP
59. Obsługa DHCP
60. Wbudowany antywirus oraz antymalware wraz z opcją zewnętrznego silnika sprawdzającego
61. Rozbudowany moduł raportowania obsługujący m.in. raportowanie ruchu sieciowego z/do danego hosta, ilość wywołań z/do danego hosta, połączenia odrzucone, połączenia zaakceptowane wraz z możliwością eksportu raportów do plików .csv/.txt
62. Wysyłanie na maila informacji o zaistniałych zagrożeniach/zdarzeniach
63. Panel aktualnego: stanu urządzenia, aktywnych połączeń VPN, połączeń klientów zdalnych, połączeń do urządzenia
64. Funkcje diagnostyczne
65. Blokowanie i ochrona stron www – możliwość tworzenia polis dostępowych/kategorii wraz z dostosowywaniem akcji (blokowanie, ostrzeżenie, informacja), obsługa białej/czarnej listy, obsługa wyjątków oraz wyłączeń, obsługa blokowania plików o określonych rozszerzeniach
66. Automatyczna aktualizacja listy blokowanych stron pobierana z pliku .txt z zewnętrznego hosta (http://hole.cert.pl/domains/domains.txt)
67. Obsługa web proxy, SNMP, SMTP Relay
68. Kontrola aplikacji – możliwość monitorowania używania aplikacji
69. Automatyczne tworzenie kopii konfiguracji zabezpieczonej hasłem na zasobie zewnętrznym
70. Możliwość tworzenia profilów: harmonogramów, godzin dostępów, limitów użytkowania internetu, limitów danych, odszyfrowywania, połączeń IPSec, dostępów do urządzenia)
71. Możliwość tworzenia list: hostów IP, grup hostów IP, hostów MAC, hostów FQDN, grup hostów FQDN, grup lokalizacyjnych, usług, grup usług)
72. Możliwość tworzenia list ACL (dla użytkowników/ grup/ połączeń VPN)
73. Możliwość ręcznego ustawienia portu dostępowego do urządzenia oraz portu dostępu do portalu użytkownika
74. Możliwość ustawienia kontroli złożoności hasła dostępowego do urządzenia dla różnych grup użytkowników
75. Automatyczna aktualizacja bibliotek urządzania wraz z możliwością zarządzania wersją firmware’u urządzania
76. Blokowanie wysyłania informacji poufnych w tle z już zainfekowanych komputerów
77. **Urządzenie dostępowe dla urządzeń serwisowych – w hali serwisowej w lokalizacji przy siedzibie głównej**
78. Wbudowane mechanizmy ochrony sieci
79. Wbudowane mechanizmy wykrywania zagrożeń oraz ochrony przed nimi
80. Wbudowane mechanizmy zapobiegające włamaniom i atakom (DoS, DDos, skanowanie portów)
81. Dostęp do urządzenia przez SSH, https, dedykowany portal
82. Możliwość konfiguracji routingów (static, OSPF, BGP, multicast)
83. Tworzenie reguł firewalla dla określonych połączeń/typów połączeń VPN/LAN/WAN/DMZ
84. Tworzenie reguł NAT oraz przekierowywań
85. Inspekcja ruchu SSL/TSL
86. Ochrona przed atakami Zero-day
87. Śledzenie połączeń: FTP, IRC, PPTP, TFTP
88. Obsługa DHCP
89. Wbudowany antywirus oraz antymalware
90. Rozbudowany moduł raportowania obsługujący m.in. raportowanie ruchu sieciowego z/do danego hosta, ilość wywołań z/do danego hosta, połączenia odrzucone, połączenia zaakceptowane wraz z możliwością eksportu raportów do plików .csv/.txt
91. Wysyłanie na maila i SMS informacji o zaistniałych zagrożeniach/zdarzeniach
92. Panel aktualnego: stanu urządzenia, aktywnych połączeń VPN, połączeń klientów zdalnych, połączeń do urządzenia
93. Funkcje diagnostyczne
94. Blokowanie i ochrona stron www – możliwość tworzenia polis dostępowych/kategorii wraz z dostosowywaniem akcji (blokowanie, ostrzeżenie, informacja), obsługa białej/czarnej listy, obsługa wyjątków oraz wyłączeń, obsługa blokowania plików o określonych rozszerzeniach
95. Automatyczna aktualizacja listy blokowanych stron pobierana z pliku .txt z zewnętrznego hosta (http://hole.cert.pl/domains/domains.txt)
96. Obsługa web proxy, SNMP, SMTP Relay
97. Kontrola aplikacji – możliwość monitorowania używania aplikacji
98. Automatyczne tworzenie kopii konfiguracji zabezpieczonej hasłem na zasobie zewnętrznym
99. Możliwość tworzenia list ACL (dla użytkowników/ grup/ połączeń VPN)
100. Możliwość ręcznego ustawienia portu dostępowego do urządzenia oraz portu dostępu do portalu użytkownika
101. Możliwość ustawienia kontroli złożoności hasła dostępowego do urządzenia dla różnych grup użytkowników
102. Automatyczna aktualizacja bibliotek urządzania wraz z możliwością zarządzania wersją firmware’u urządzania
103. Blokowanie wysyłania informacji poufnych w tle z już zainfekowanych komputerów
104. Urządzenie ma pracować jako punkt dostępu urządzeń serwisowych z systemami operacyjnymi o skończonym wsparciu technicznym producenta (Windows XP, Windows 7, Windows 8 i inne) do internetu poprzez wbudowany w urządzenie moduł Wi-Fi.
105. Urządzenie ma obsługiwać urządzenia zewnętrzne wyposażone w moduły WiFi o standardach 802.11: b, a, g, n.