Znak sprawy BGP.271.9.2022

SWZ załącznik nr 3

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
7. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).

10. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)

11. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
12. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
13. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
14. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
15. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej.
16. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
17. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych
    i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
18. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

19. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
20. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
21. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
22. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

23. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
24. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
25. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
26. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

27. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
28. Ochrona antyspam ma działać w oparciu o:
    a) białe/czarne listy,
    b) DNS RBL,
    c) heurystyczny skaner.

29. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
30. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE (VPN)

31. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
32. Odpowiednio kanały VPN można budować w oparciu o:
    a) PPTP VPN,
    b) IPSec VPN,
    c) SSL VPN.
33. SSL VPN musi działać w trybach Tunel i Portal.
34. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
35. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
36. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
37. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

38. Urządzenie ma posiadać wbudowany filtr URL.
39. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
40. Administrator musi mieć możliwość dodawania własnych kategorii URL.
41. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.

42. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
43. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
    a) blokowanie dostępu do adresu URL,
    b) zezwolenie na dostęp do adresu URL,
    c) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
47. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

49. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
    a) lokalną bazę użytkowników (wewnętrzny LDAP),
    b) zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c) usługę katalogową Microsoft Active Directory.
50. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
51. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
    a) SSL,
    b) Radius,
    c) Kerberos.
52. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.

53. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

55. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a) równoważenie względem adresu źródłowego,
    b) równoważenie względem połączenia.
57. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
59. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
60. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
61. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
62. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

63. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.

64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS.
67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
68. Urządzenie musi posiadać usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM

69. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
70. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
71. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
72. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
73. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
74. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
75. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
76. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
77. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.

78. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
79. Urządzenie musi posiadać funkcjonalność anonimizacji logów.
80. Urządzenie ma mieć możliwość bezpośredniego podłączenia karty pamięci typu SD w celu zbierania logów.

RAPORTOWANIE

81. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
82. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
83. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
84. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.
85. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
86. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
87. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy.

PARAMETRY SPRZĘTOWE

88. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash.
89. Liczba portów Ethernet 10/100/1000Mbps – min. 8.

90. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.
91. Przepustowość Firewall – min. 4 Gbps.
92. Przepustowość Firewall wraz z włączonym systemem IPS – min. 2,4 Gbps.
93. Przepustowość filtrowania Antywirusowego – min. 495 Mbps.
94. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps.
95. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100.
96. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20.
97. Obsługa min. VLAN 64.
98. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
99. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
100. Urządzenie jest nielimitowane na użytkowników.

LICENCJE

101. Urządzenie musi zostać dostarczone w min. roczną aktualizacją dostarczanych modułów oraz min. roczną gwarancją.

Urządzenie musi być dostarczone do zamawiającego i zainstalowane oraz skonfigurowane na miejscu. Dodatkowo dostawca przeszkoli administratora systemów IT Zamawiającego w zakresie obsługi dostarczonego Urządzenia.