Załącznik Nr 2 do Zapytania ofertowego

CEM.ZP.261.38/15

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Urządzenie pełniące funkcje ściany ogniowej i bramy VPN

1.1. Architektura urządzenia

1.1.1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
1.1.2. Urządzenie musi posiadać wbudowane co najmniej 8 miedzianych portów 1000BASE-T.
1.1.3. Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych – minimum 40 sieci VLAN.
1.1.4. Urządzenie musi posiadać dedykowany dla zarządzania port konsoli.
1.1.5. Urządzenie musi posiadać dedykowany dla zarządzania port Ethernet 10/100/1000 (Out-of-Band Management).
1.1.6. Urządzenie musi posiadać co najmniej 1 port USB 2.0 i umożliwiać podłączenie do niego zewnętrznej pamięci flash do kopiowania plików z i na wewnętrzną pamięć flash urządzenia.
1.1.7. Urządzenie musi być wyposażone w co najmniej 8GB pamięci flash.
1.1.8. Urządzenie musi być wyposażone w co najmniej 8GB pamięci RAM.
1.1.9. Urządzenie musi być wyposażone w co najmniej 80GB dysk twardy.

1.2. Obudowa

1.2.1. Urządzenie ma możliwość instalacji w szafie typu rack 19".
1.2.2. Wysokość urządzenia nie większa niż 1RU
1.2.3. Urządzenie musi być przystosowane do pracy w zakresie temperatur 5-40 stopni Celsjusza
1.2.4. Urządzenie na panelu czołowym musi posiadać świetlną sygnalizację co najmniej następujących stanów urządzenia:
  1.2.4.1. wystąpiła awaria zasilacza,
  1.2.4.2. wystąpiła krytyczna awaria urządzenia

1.3. Wydajność urządzenia

1.3.1. Przepustowość teoretyczna firewall'a dla ruchu IPv4 i ruchu IPv6 musi być na poziomie 950 Mb/s, a dla ruchu rzeczywistego (tzw. ruch multiprotocol) nie mniej niż 450 Mb/s.
1.3.2. Urządzenie musi obsługiwać co najmniej 9.000 nowych połączeń na sekundę.
1.3.3. Urządzenie musi obsługiwać co najmniej 90.000 równoczesnych połączeń.
1.3.4. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 160Mbps.
1.3.5. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 90 tuneli VPN wykorzystujących IPsec.

1.4. Funkcjonalność urządzenia

1.4.1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
1.4.2. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji .
1.4.3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
1.4.4. Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP.
1.4.5. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access).

1.4.6. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.
1.4.7. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256.
1.4.8. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 .
1.4.9. Urządzenie musi obsługiwać protokół Diffiego-Hellmana .
1.4.10. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN.
1.4.11. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu).
1.4.12. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI.
1.4.13. Urządzenie obsługuje protokół NTP.
1.4.14. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego.
1.4.15. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6.
1.4.16. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
1.4.17. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:
1.4.17.1. Hypertext Transfer Protocol (HTTP),
1.4.17.2. File Transfer Protocol (FTP),
1.4.17.3. Extended Simple Mail Transfer Protocol (ESMTP),
1.4.17.4. Domain Name System (DNS),
1.4.17.5. Simple Network Management Protocol v 2/3 (SNMP),
1.4.17.6. Internet Control Message Protocol (ICMP),
1.4.17.7. SQL*Net,
1.4.18. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP.
1.4.19. Urządzenie zapewnia wsparcie stosu protokołów IPv6 .
1.4.20. Urządzenie obsługuje routing statyczny i dynamiczny (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
1.4.21. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu.
1.4.22. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
1.4.22.1. źródłowy i docelowy adres IPv4
1.4.22.2. źródłowy i docelowy adres IPv6
1.4.22.3. źródłowy i docelowy numer portu UDP
1.4.22.4. źródłowy i docelowy numer portu TCP
1.4.23. Urządzenie nie może posiadać żadnych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.

1.5. Funkcjonalność urządzenia – NGFW

1.5.1. Urządzenie musi zapewniać funkcjonalności tzw. Next-Generation firewall w zakresie nie mniejszym niż:
1.5.1.1. system automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control);
1.5.1.2. system IPS;
1.5.1.3. system ochrony przed malware;
1.5.1.4. system filtracji ruchu w oparciu o URL.

1.5.2. System wykrywania aplikacji AVC musi:
1.5.2.1. Posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych.
1.5.2.2. Zapewniać wydajność co najmniej 250Mbps.

1.5.3. System IPS musi:

1.5.3.1. Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
1.5.3.2. Posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu).
1.5.3.3. System IPS powinien pozwalać na pracę z przepustowością co najmniej 125Mbps przy jednoczesnym działaniu AVC.

1.5.4. System filtracji URL musi:

1.5.4.1. Pozwalać na kategoryzację stron – w co najmniej 70 kategoriach.
1.5.4.2. Zapewniać bazę URL o wielkości nie mniejszej niż 250 mln URL.

1.5.5. System musi posiadać wbudowany podsystem wykrywania oprogramowania złośliwego (malware) poprzez:

1.5.5.1. Sprawdzenie reputacji plików w systemie globalnym.
1.5.5.2. Sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze).
1.5.5.3. Narzędzia analizy historycznej dla plików przesłanych w przeszłości a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).
1.5.5.4. Wykrywanie ataków Zero-Day.

1.5.6. System musi zapewniać **centralną konsolę zarządzania** zapewniającą informacje ogólne i szczegółowe o:

1.5.6.1. Wykrytych hostach.
1.5.6.2. Aplikacjach.
1.5.6.3. Zagrożeniach i atakach.
1.5.6.4. Wskazaniach kompromitacji (indication-of-compromize) na podstawie:
1.5.6.4.1. Zdarzeń z IPS.
1.5.6.4.1.1. Malare backdoors.
1.5.6.4.1.2. Exploit kits.
1.5.6.4.1.3. Ataków na aplikacje webowe.
1.5.6.4.1.4. Połączenia do serwerów Command'n'Control.
1.5.6.4.1.5. Wskazań eskalacji uprawnień.
1.5.6.4.2. Zdarzeń sieciowych.
1.5.6.4.2.1. Połączeń do znanych adresów IP Command'n'Control.
1.5.6.4.3. Zdarzeń związanych z malware.
1.5.6.4.3.1. Wykrycie malware.
1.5.6.4.3.2. Wykrycie infekcji dropperów.

1.6. Zarządzanie i konfiguracja

1.6.1. Urządzenie musi umożliwiać zarządzanie:
1.6.1.1. Przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
1.6.1.2. Przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji.
1.6.1.3. Przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji.
1.6.2. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.
1.6.3. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
1.6.4. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.
1.6.5. Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
1.6.6. Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.
1.6.7. Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954).
1.6.8. Dostęp do urządzenia jest możliwy przez SSH.

1.6.9. Urządzenie obsługuje protokół SNMP v 2/3.

1.6.10. Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.

1.6.11. Urządzenie umożliwia zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych.

1.6.12. Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP.

1.6.13. Urządzenie musi posiadać zaawansowaną instrumentację pozwalającą na uzyskanie szczegółowej informacji o obciążeniu CPU przez każdy z procesów oddzielnie, z podziałem na procesy, w interwałach czasowych 5 minut, 1 minuta i 5 sekund.

1.7. Wymagana ilości urządzeń:

1.7.1. Urządzenie pełniące funkcje ściany ogniowej i bramy VPN - 2 sztuki.

1.7.2. Oprogramowanie centralnej konsoli do zarządzania do NGFW powinno być dostarczona z licencja do zarzadzania minimum 2 systemami ściany ogniowej – 1 sztuka.

1.8. Wdrożenie:

1.8.1. Według wytycznych zamawiającego z przeszkoleniem pracowników w zakresie eksploatacji.

1.9. Wymagania dla inżynierów do wdrożenia:

1.9.1. Do wdrożenia systemy wymagane jest posiadanie inżynierów, którzy posiadają ważne od min 1 roku certyfikację na poziomie (Do oferty należy załączyć odpowiednie certyfikaty) CCNP, CCDP, CCNA Security.

1.9.2. **Gwarancja i serwis**

Urządzenie pełniące funkcje ściany ogniowej i bramy VPN musi być objęte co najmniej **1 rocznym** serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

Cały sprzęt ma pochodzić z autoryzowanego kanału dystrybucji na rynek Polski. Zamawiający ma mieć prawa licencyjne do oprogramowania.

Centralna konsola zarzadzania NGFW musi być objęte **co najmniej 3 letnim** serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD do wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

W ramach w/w serwisu należy zapewnić dostęp do aktualizacji do systemów:

- automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)
- IPS
- ochrony przed malware
- filtracji ruchu w oparciu o URL
- centralna konsoli do zarządzania NGFW
przez okres 3 lat