Opis Przedmiotu Zamówienia

na "modernizację infrastruktury urządzeń bezpieczeństwa klasy UTM w Urzędzie Miasta Płocka w ramach poprawy poziomu bezpieczeństwa teleinformatycznego komórek organizacyjnych UMP"

Przedmiot zamówienia dotyczy modernizacji części infrastruktury teletechnicznej w Urzędzie Miasta Płocka funkcjonującej na styku sieci wewnętrznych i dostępu do internetu. Są to urządzenia klasy UTM wraz z przyległymi przełącznikami sieciowymi.
W zakres modernizacji wchodzi:

1. dostawa nowych urządzeń i licencji na zwiększenie dziennej quoty na obecnym systemie zarządzania logami i jego upgradem do najnowszej wersji – maszyna wirtualna
2. wymianie wyeksploatowanych aktywnych urządzeń sieciowych na nowe i przeniesieniem obecnej konfiguracji / funkcjonalności.

Zadanie ma na celu podniesienie standardu bezpieczeństwa teleinformatycznego Urzędu Miasta Płocka.

Sprzęt który podlega wymianie:

1. Fortigate-600C (Firmware Version v5.0,build0292) - 2 szt
2. Cisco 6509E (Version 12.2(17r)S4) - 1 szt
3. Cisco 3845 - (Version 12.4(9)T1) - 1 szt

Maszyna wirtualna do upgradu do najnowszej wersji

1. FortiAnalyzer VM64 (Firmware Version v5.0.7-build0321) - 1 szt

Zakup licencji:

1. dodatkowe 3GB/dzień zwiększające quotę logów na FortiAnalyzer VM64 z 2 GB na 5 GB/dzień

Dostawa nowego sprzętu:

I. SYSTEM UTM W POSTACI REDUNDANTNEJ

Wymagania Ogólne systemu:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Wykonawca dostarczy odpowiednią ilość wkładek SFP+ 10GBASE-SR i/lub SFP+ 10GBASE-LR niezbędną do wykonania fizycznych połączeń do przełączników typu 1 i wkładki SFP 1000BASE-SX lub SFP 1000BASE-LX niezbędne do utworzenia połączeń HA typu „heartbeat" i uruchomienia systemu.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w podwójne zasilanie AC (dual PS).

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 15 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 10 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall:

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware vCenter (ESXi).

Połączenia VPN:

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN:

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem:

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie:

maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware:

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami:

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DdoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji:

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW:

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków –

białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji:

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie:

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. System powinien być zgodny z posiadaną przez Zamawiającego platformą centralnego logowania i raportowania firmy Fortinet Fortianalyzer VM64.
3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5. Musi istnieć możliwość logowania do serwera SYSLOG.

Kontroler sieci bezprzewodowej:

1. System musi zapewnić centralną obsługę urządzeń Access Point Fortinet FortiAP-223B

(FAP-223B-E), które posiada Zamawiający

Certyfikaty:

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje:

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie:

System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

II. PRZEŁĄCZNIK LAN (typ 1) – 2 szt

Wymagania Ogólne:

Dostarczone przełączniki po wdrożeniu mają stanowić warstwę rdzenia sieci z pełną redundancją. Połączenie między mini 2 x 40Gbps STACK ma zapewnić możliwość tworzenia połączeń typu LACP z dowolnego urządzenia accesowego. Mają być zlokalizowane w różnych serwerowniach połączonych między sobą światłowodem jedno i wielomodowym OM4 o długości wg pomiaru 228 mb.
Wykonawca dostarczy odpowiednią ilość wkładek SFP+ 10GBASE-SR i/lub SFP+ 10GBASE-LR i QSFP+ 40GBASE-LR4 niezbędną do wykonania fizycznych połączeń i uruchomienia systemu plus dodatkowo po 8 szt wkładek SFP+ 10GBASE-T na każde urządzenie.

Parametry:

1. Typ i liczba portów:
   - Minimum 48 portów 1G/10G SFP+ umieszczonych z przodu obudowy
   - Minimum 6 portów 40GbE QSFP+ umieszczonych z przodu obudowy
   - Wszystkie porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo
2. Wbudowany, dodatkowy, dedykowany port Gigabit Ethernet do zarządzania poza pasmem - out of band management
3. Port konsoli RS232 ze złączem DB9 lub RJ45
4. Port USB 2.0
5. Wydajność: minimum 1440 Gbps (prędkość przełączania „wirespeed” dla każdego portu przełącznika)
6. Przełączanie w warstwie 2 i 3 modelu OSI
7. Wielkość bufora pakietów (packet buffer): minimum 16MB
8. Minimum 64GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash)
9. Oparty o jądro Linux Bootloader powinien znajdować się na niezależnym od właściwego systemu operacyjnego nośniku pamięci.
10. Oprócz uruchamiania systemu operacyjnego Bootloader musi pozwalać na: dostęp do logów, zrzutów pamięci (coredump) i konfiguracji, naprawę i formatowanie przestrzeni pamięci, wygrywanie i aktualizację systemu operacyjnego, czyszczenie konfiguracji,

czyszczenie i zmianę haseł administratorskich, wybór wersji systemu operacyjnego
11. Minimum 16GB pamięci operacyjnej
12. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów)
13. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Nie dopuszczalne są rozwiązania, z mieszanym przepływem powietrza.
14. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
15. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
16. Tablica adresów MAC o wielkości minimum 90000 pozycji
17. Obsługa ramek Jumbo o wielkości co najmniej 9kB
18. Obsługa Quality of Service
19. Obsługa mechanizmów, co najmniej: strict priority (SP) queuing, Deficit weighted round robin (DWRR) queuing
20. Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol
21. Obsługa sieci IEEE 802.1Q VLAN – 4000 jednoczesnych sieci VLAN
22. Obsługa IGMP v2/v3, IGMP Snooping, PIM SM
23. Routing IPv4 – statyczny i dynamiczny (min. OSPF, BGP)
24. Routing IPv6 – statyczny i dynamiczny (min. OSPFv3)
25. Obsługa ECMP (Equal Cost Multi Path)
26. Obsługa VRRP
27. Obsługa tunelowania GRE
28. Obsługa Virtual Routing and Forwarding (VRF), ze wsparciem dla co najmniej 8 instancji VRF
29. Tablica routingu o pojemności co najmniej 120000 wpisów dla IPv4 oraz co najmniej 32000 wpisów dla IPv6
30. Obsługa funkcji klienta DHCP
31. Obsługa DHCP Relay dla IPv4 i IPv6
32. Obsługa list ACL (co najmniej 16000) na bazie informacji z warstw 2 i 3 modelu OSI. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
33. Obsługa standardu 802.1p
34. Funkcja ograniczania ruchu typu multicast i broadcast
35. Funkcja kopiowania ruchu wejściowego i wyjściowego (port mirroring) lokalnego (w obrębie urządzenia)
36. Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS oraz TACACS+
37. Zarządzanie poprzez port konsoli (CLI), SNMP 2c, SNMP 3, interfejs graficzny (WebGUI) znajdujący się bezpośrednio na urządzaniu oraz SSH v2
38. Obsługa Syslog
39. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
40. Obsługa sFlow
41. Obsługa Network Time Protocol (NTP)
42. Obsługa Secure FTP (SFTP) oraz TFTP
43. Obsługa skryptów w języku Python
44. Obsługa REST API
45. Obsługa RMON (minimum grupy 1, 2, 3 i 9)
46. Obsługa funkcji diagnostycznych ping i traceroute dla IPv4 i IPv6
47. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
48. Przechowywanie co najmniej dwóch wersji oprogramowania na przełączniku
49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
50. Parametr Mean Time Between Failures (MTBF) wynoszący co najmniej 30 lat
51. Wysokość w szafie 19” – 1U o głębokości maksymalnie 55 cm
52. Maksymalny pobór mocy nie większy niż 360W

53. Minimalny zakres temperatur pracy od 0°C do 40°C
54. Urządzenia muszą pochodzić z oficjalnego kanału dystrybucji na Polskę.
55. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji.

III. PRZEŁĄCZNIK LAN (typ 2) – 1 szt

Wymagania Ogólne:

Dostarczony przełącznik po wdrożeniu ma stanowić warstwę accesową przejętą z przełącznika cisco Catalyst 6509E. Wykonawca dostarczy odpowiednią ilość wkładek SFP+ 10GBASE-SR i/lub SFP+ 10GBASE-LR niezbędną do wykonania fizycznych połączeń do przełączników typu 1 i uruchomienia systemu

1. Minimum 48 portów gigabitowych w standardzie 100/1000BaseT
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 112 Mp/s
5. Tablica adresów MAC o wielkości minimum 32000 pozycji
6. Obsługa ramek Jumbo
7. Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
8. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
9. Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
10. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
11. Obsługa VxLAN
12. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
13. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN
14. Funkcja Root Guard oraz BPDU protection
15. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania.
16. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
17. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping
18. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
19. Obsługa standardu 802.1p – min. 8 kolejek na porcie
20. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
21. Funkcja autoryzacji użytkowników zgodna z 802.1x
22. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
23. RADIUS Accounting
24. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3
25. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
26. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https

27. Obsługa Syslog
28. Obsługa NTP lub SNTPv4
29. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku
30. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
31. Wsparcie dla funkcji Private VLAN lub równoważnego
32. Obsługa protokołu VTP lub MVRP
33. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego
34. Minimalny zakres pracy od 0°C do 45°C
35. Wysokość w szafie 19" – 1U, głębokość nie większa niż 30 cm
36. Maksymalny pobór mocy nie większy niż 190W
37. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
38. Urządzenia muszą pochodzić z oficjalnego kanału dystrybucji na Polskę
39. Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 5 lat od daty zakończenia produkcji urządzenia) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia.

Zakres wdrożenia:

System bezpieczeństwa musi zapewnić pełną redundancję sieci poprzez rozlokowanie urządzeń w 2 serwerowniach, które są połączone między sobą światłowodem jednomodowym (według pomiaru 228 mb) i wielomodowym OM4 (według pomiaru 223 mb). Na przełącznicy światłowodowej jest wolnych 8 włókien jednomodowych i 8 włókien wielomodowych.

Zabezpieczenie sieci Zamawiającego:

- Dokonanie instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.
- Wykonawca dostarczy odpowiednią ilość wkładek SFP, SFP+ i QSFP+, patchcordów światłowodowych i UTP niezbędną do wykonania fizycznych połączeń.
- Analiza oraz przeniesienie aktualnej konfiguracji UTM-a, optymalizacja, a w przypadku braku odpowiednich funkcjonalności - ponowna konfiguracja.
- Analiza oraz przeniesienie funkcjonalności przełącznika Cisco Catalyst 6509E i Cisco 3845, na nowego UTM-a

Firewall - UTM:

- W konfiguracji urządzeń UTM muszą zostać włączone / skonfigurowane min. usługi / funkcjonalności:
  - klaster HA,
  - ochrony przed atakami typu DoS/DDoS, itp.,
  - ochrony antywirusowej,
  - web filter,
  - Intrusion prevention,
  - DLP w podstawowej funkcjonalności,
  - Application control,
  - SSL inspection,
  - Utworzenie konfiguracji serwera VPN (integracja kont użytkowników z Active Directory) i odtworzenie 4 połączeń zdalnych VPN przez Ipsec do urządzeń Fortigate 60D,
  - przeniesienie konfiguracji dla FortiAP - 6 szt (4 sieci WiFi),
  - technologia SD-WAN dla 2 łączy internetowych,

- 3 łącze internetowe przez modem LTE na potrzeby managementu przez VPN (modem z aktywną kartą sim dostarczy Zamawiający),
- podłączenie do FortiAnalyzera,
- integracja z Sandboxem,

- Instalowane urządzenie musi chronić zainstalowane wewnątrz sieci Zamawiającego, serwery aplikacyjne [głównie przed atakami typu DoS, sql-injection, itp].

Przełączniki LAN:

- Instacja switchy przełączników CORE, upgrade, konfiguracja połączenia typu stack.
- Konfiguracja dostępu SSH, VLAN, loop protect, STP, UDLD, arp protect, trunks.
- Instacja switchy przełącznika dostępowego, upgrade, konfiguracja dostępu SSH,VLAN, loop protect, STP, UDLD, arp protect, dhcp spoofnig, trunks.
- Podłączenie przełącznika dostępowego do CORE.

FortiAnalyzer VM64:

- Upgrade maszyny wirtualnej FortiAnalyzer VM64 do najnowszej wersji.
- Zwiększenie quoty do 5GB / dzień
- Podłączenie FortiAnalyzera VM64 do obecnego serwera poczty Fortimai VM04 (Firmware version: v6.2)
- Ponowna konfiguracja w celu poprawnego zbierania logów z nowego systemu UTM

Szkolenia:

Wykonawca przeprowadzi jednodniowe szkolenie dla 3 administratorów sieci w siedzibie Zamawiającego z obsługi wdrażanego systemu.

Stare (wymieniane) urządzenia pozostają w Urzędzie Miasta Płocka