Szczegółowy opis przedmiotu zamówienia

I. System ochrony poczty

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware bez limitu licencyjnego na ilość chronionych kont użytkowników lub być dostarczony z licencjami na pełną pojemność rozwiązania. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej, Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania, rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z wskazanych trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi być wyposażony w interfejsy: 4 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1,8.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty, umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL
   (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail - z wykorzystaniem protokołu SSL
   (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2, oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 100 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 000 wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
19. Możliwość integracji z Office 365 oraz serwerami Exchange z wykorzystaniem API.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną

platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu virus-outbreak.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antyspamowej.
13. Ochrona typu outbreak.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.
5. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją

wstawienia własnego logo firmy.

3. Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.

Certyfikaty

VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę Antyspam, URL Filtering, kontrolę antywirusową, ochronę typu Virus Outbrake, Sandboxing w chmurze, ochronę typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

Wdrożenie

Wykonawca dokona montażu rozwiązania we wskazanych przez Zamawiającego zasobach rack. Dokonana musi zostać aktualizacja do najnowszej stabilnej i sugerowanej przez producenta wersji firmware, oprogramowania oraz zainstalowane wszystkie niezbędne łatki. Konfiguracja w ramach rozwiązania dotyczyć będzie wskazanych do dostarczenia funkcjonalności z uwzględnieniem wskazanych przez Zamawiającego reguł, logiki oraz sposobu obsługi ruchu w istniejącym obecnie środowisku Zamawiającego bazującym na Cisco Ironport ESA oraz maszynach C170-K9.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 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. Punkt dostępowy (AP) - 30 sztuk

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Urządzenie musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia minimum w następujących warunkach klimatycznych:
   Temperatura pracy 0-47°C;
   Wilgotność 5-90%;
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
   a) 2.4 GHz 802.11b/g/n/ax;
   b) 5GHz 802.11a/n/ac/ax z szerokościami kanałów 20Mhz, 40MHz, 80MHz;

   c) 2.4/5GHz skaner spectrum;
4. Urządzenie musi być wyposażone w moduł radiowy Bluetooth/BLE.
5. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 12 SSID.
6. Liczba interfejsów:
   a) 2x Ethernet w standardzie 10/100/1000 Base-TX
      oraz przynajmniej jedno z nich w standardzie 2500 Base-TX
   b) Port szeregowy RS-232 poprzez RJ-45 lub USB
   c) Port USB 2.0

7. Możliwość zasilania urządzenia poprzez oba interfejsy ETH w standardzie 802.3af/at lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   a) Tunnel,
   b) Bridge,
   c) Mesh.
9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a) MIMO - 2x2 , 1x1 w przypadku radia pracującego jako skaner
    b) Transmit Beam Forming (TxBF),
    c) Maksymalna przepustowość dla poszczególnych modułów radiowych:
       570 Mbps oraz 1200 Mbps;
    d) Wymagana moc nadawania: min. 20 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm; min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    e) Wsparcie dla 802.11n 20/40Mhz HT,
    f) Anteny - 3 wewnętrzne dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
    g) Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
    h) Maksymalna deklarowana liczba klientów per moduł radiowy - 512.
11. Funkcje interfejsu radiowego:
    a) Skaner częstotliwości 2.4 oraz 5 GHz,
    b) Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
    c) Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,
12. Funkcje dodatkowe:
    a) Low-Density Parity Check (LDPC) Encoding,
    b) Maximum Likelihood Demodulation (MLD),
    c) Maximum Ratio Combining (MRC),
    d) A-MPDU and A-MSDU Packet Aggregation,
    e) MIMO Power Save,
    f) Short Guard Interval,

g) WME Multimedia Extensions.

13. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance oraz posiadać certyfikację DFS.
14. Współpraca z kontrolerem:
    a) Urządzenia mają być kompatybilne z UTM Fortinet posiadanym przez zamawiającego.
    b) Jako rozwiązanie równoważne dopuszcza się dostarczenie klastra HA urządzeń/kontrolerów w formie dedykowanej platformy sprzętowej (spełniającej wszystkie funkcjonalności dostępne dla Zamawiającego w platformie referencyjnej jaką jest posiadane rozwiązanie bazujące na urządzeniach Fortigate) oraz niezbędnych licencji, jednakże Zamawiający wymaga dedykowanego szkolenia w zakresie dostarczanego rozwiązania dla jednej osoby w wymiarze minimum 40 godzin.

Dedykowane zasilacze sieciowe do specyfikowanych punktów dostępowych

Do specyfikowanych punktów dostępowych Wykonawca dostarczy 24 szt. dedykowanych zasilaczy sieciowych 230V/50Hz.

Gwarancja oraz wsparcie dla punktów dostępowych

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji, oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 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.

Wdrożenie

W ramach wdrożenia Wykonawca dokona konfiguracji środowiska tożsamo z istniejącym środowiskiem obecnie posiadanym przez Zamawiającego. Skonfigurowane muszą zostać wszystkie niezbędne ustawienia dostępu, uwierzytelniania, polityka radiowa. Przygotować należy wszystkie niezbędne elementy w kontrolerze do podłączenia nowych AP z uwzględnieniem ewentualnej pracy równoległej obu rozwiązań.