BYTOMSKIE PRZEDSIĘBIORSTWO KOMUNALNE
Spółka z o.o.
41-902 Bytom, pl. T. Kościuszki 11
tel. (32) 39-67-119
DZIAŁ INFORMATYKI

Specyfikacja istotnych warunków zamówienia dla zadania:

Zakup urządzenia UTM (zintegrowana ochrona sieci)

Przedmiotem zamówienia jest urządzenie klasy UTM (Unified Threat Management) wraz z usługą wdrożenia i gwarancją.

1. Wymagania dotyczące urządzenia

Urządzenie posiada zintegrowaną architekturę bezpieczeństwa i ma posiadać poniższe funkcje:

1.1. ZAPORA KORPORACYJNA (Firewall)

1.1.1. Firewall klasy Stateful Inspection.

1.1.2. Urządzenie ma obsługiwać translacje adresów NAT, PAT, 1-PAT.

1.1.3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).

1.1.4. Interface (GUI) do konfiguracji firewalla 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.

1.1.5. Administrator ma możliwość zdefiniowania minimum 10 różnych zestawów reguł na firewall'u.

1.1.6. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).

1.1.7. 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).

1.2. INTRUSION PREVENTION SYSTEM (IPS)

1.2.1 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.

1.2.2 Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.

1.2.3 Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

1.2.4 Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.

1.2.5 Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.

1.2.6 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.

1.3. KSZTAŁTOWANIE PASMA (Traffic Shapping)

1.3.1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytezację ruchu oraz minimalną i maksymalną wartość pasma.

1.3.2. Ograniczenie pasma lub priorytezacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

1.3.3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

1.4. OCHRONA ANTYWIRUSOWA

1.4.1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

1.4.2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.

1.4.3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

1.4.4. 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.

1.5. OCHRONA ANTYSPAM

1.5.1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

1.5.2. Ochrona antyspam ma działać w oparciu o:
   a. białe/czarne listy,
   b. DNS RBL,
   c. heurystyczny skaner.

1.5.3. 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.

1.5.4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

1.6. WIRTUALNE SIECI PRYWANTE (VPN)

1.6.1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

1.6.2. Odpowiednio kanały VPN można budować w oparciu o:
   a. PPTP VPN,
   b. IPSec VPN,
   c. SSL VPN.

1.6.3. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

1.6.4. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.

1.7. FILTR ADRESÓW URL

1.7.1. Urządzenie ma posiadać wbudowany filtr URL.

1.7.2. Filtr URL ma działać w oparciu o klasyfikację URL dostarczaną przez producenta rozwiązania zawierającą co najmniej 50 kategorii tematycznych stron internetowych.

1.7.3. Administrator musi mieć możliwość dodawania własnych kategorii URL.

1.7.4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.

1.7.5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.

1.7.6. 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.

1.7.7. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.

1.7.8. Możliwość identyfikacji oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.

1.7.9. Możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

1.8. UWIERZYTELNIANIE

1.8.1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
   a. lokalną bazę użytkowników (wewnętrzny LDAP),
   b. zewnętrzną bazę użytkowników (zewnętrzny LDAP) ,
   c. integracje z serwerem Microsoft Active Directory.

1.8.2. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
   a. SSL,
   b. Radius,
   c. Kerberos.

1.8.3. Autoryzacja użytkowników z wykorzystaniem użytkowników Microsoft Active Directory nie wymaga instalacji agenta na serwerze AD ani modyfikacji schematu domeny.

1.9. ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).

1.9.1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

1.9.2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   a. równoważenie względem adresu źródłowego,
   b. równoważenie względem adresu źródłowego i docelowego (połączenia).

1.9.3. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

1.10. POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

1.10.1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci

1.10.2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay

1.10.3. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.

1.10.4. Urządzenie musi posiadać usługę klienta NTP.

1.10.5. Urządzenie musi posiadać DNS Proxy.

1.10.6. Urządzenie musi być wyposażone w pasywny skaner sieci wykrywający podatności.

1.11. ADMINISTRACJA URZĄDZENIEM

1.11.1. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.

1.11.2. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

1.11.3. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.

1.11.4. Komunikacja może odbywać się na porcie innym niż https (443 TCP).

1.11.5. Urządzenie może być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

1.11.6. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).

1.12. RAPORTOWANIE

1.12.1. Urządzenie ma być dostarczone wraz z dedykowanym systemem do raportowania.

1.12.2. Narzędzie raportujące musi być oparte o darmowy system np. system z rodziny Linux.

1.12.3. Interfejs użytkownika musi być dostępny poprzez przeglądarkę internetową.

1.12.4. Interfejs użytkownika narzędzia raportującego ma być dostępny co najmniej w językach Polskim i Angielskim.

1.12.5. Przesyłanie logów pomiędzy urządzeniem a narzędziem raportującym musi odbywać się za pomocą protokołu syslog.

1.12.6. Narzędzie raportujące musi posiadać możliwość automatycznej aktualizacji swoich komponentów z Internetu bez ingerencji użytkownika.

1.12.7. Rozwiązanie musi posiadać możliwość wygenerowania raportów graficznych, na podstawie zebranych logów, w tym co najmniej:

a. raporty WEB zawierające informacje o co najmniej: odwiedzanych stronach WWW, ilości połączeń do tych stron, ilości pobranych danych, kategoriach tematycznych (do których należą odwiedzane strony), użytkownikach, którzy łączyli się z danymi adresami oraz adresach IP z których wchodzono na owe strony,

b. raporty pasywnego skanera sieci, zawierające informacje o co najmniej: wykrytych zagrożeniach, aplikacjach, w których zostały wykryte podatności, typach programów, w których wykryto podatności, poziomie ważności wykrytych zagrożeń,

c. raporty IPS zawierające informacje o co najmniej: wykrytych przez IPS zagrożeniach, adresach źródłowych i adresach docelowych hostów, których te zagrożenia dotyczą.

1.12.8. Raporty graficzne muszą oferować możliwość:

a. przeszukiwania zgromadzonych informacji,

b. wyświetlenia zgromadzonych informacji, dla wybranego: dnia, tygodnia, miesiąca,

c. eksportu do zewnętrznych plików obsługujących format PDF oraz CSV.

1.12.9. Narzędzie raportujące musi umożliwiać przeglądanie zgromadzonych logów, oraz dawać możliwość ich filtrowania po parametrach co najmniej takich jak: protokół, źródłowy adres IP, docelowy adres IP, port docelowy, nazwa docelowa, czas (od-do), nazwa użytkownika, akcja.

1.12.10. Przeglądarka logów musi dawać możliwość ukrycia kolumn z informacjami zbędnymi dla administratora.

1.12.11. Narzędzie raportujące musi posiadać możliwość tworzenia wielu kont użytkowników.

1.12.12. Narzędzie raportujące musi umożliwiać pracę wielu użytkowników jednocześnie.

1.12.13. Narzędzie raportujące musi być dostarczane w ramach podstawowej licencji na urządzenie, bez dodatkowych opłat.

1.13. PARAMETRY SPRZĘTOWE

1.13.1. Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 120 GB.

1.13.2. Liczba portów Ethernet 10/100/1000 – min. 8

1.13.3. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.

1.13.4. Urządzenie pozwala na użycie nie mniej niż 8 niezależnych łączy WAN.

1.13.5. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 1 000 Mbps.

1.13.6. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 250 Mbps.

1.13.7. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 500.

1.13.8. Obsługa min. 256 VLAN-ów.

1.13.9. Maksymalna liczba równoczesnych sesji wynosi min. 250 000.

1.13.10. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

1.13.11. Urządzenie jest nielimitowane na użytkowników.

2. <u>Wymagania wobec przedmiotu zamówienia:</u>

2.1 Wykonawca dostarczy przedmiotowe urządzenie fabrycznie nowe w terminie 7 dni roboczych od otrzymania zamówienia,

2.2 Wykonawca dostarczy wraz z urządzeniem dokument producenta potwierdzający zakup gwarancji w systemie tzw. NBD oraz zakup subskrypcji na wszelkie uaktualnienia urządzenia w okresie 5 lat od daty podpisania protokołu odbioru,

2.3 Po wybraniu Wykonawcy przeprowadzi On audyt obecnego u Zamawiającego urządzenia Firewall pod kątem ustawień,

2.4 Wykonawca zainstaluje urządzenie w szafie RACK Zamawiającego znajdującej się w siedzibie firmy w Bytomiu przy pl. T. Kościuszki 11,

2.5 Wykonawca wykona konfigurację urządzenia zachowując ustawienia Zamawiającego,

2.6 Wykonawca w konsultacji z Zamawiającym wykona konfigurację podstawowych oraz zaawansowanych funkcjonalności urządzenia.

2.7 Wszelkie prace wdrożeniowe muszą być wykonywane w godzinach pracy Zamawiającego tj. od poniedziałku do piątku od 8:00 do 15:00 w terminie nie później niż 5 dni roboczych od dnia dostarczenia urządzenia do Zamawiającego,

2.8 W ramach wdrożenia Wykonawca oddeleguje na jego zakończenie kompetentnego pracownika na 8 godzin w celu konsultacji i przeszkolenia pracowników Działu Informatyki pod kątem użytkowania wdrażanego urządzenia UTM.

2.9 Wykonawca dostarczy procedurę zgłoszenia serwisowego umożliwiającego zgłaszanie usterek telefonicznie lub poprzez pocztę e-mail. codziennie w dni robocze od 8:00 do 15:00.

2.10 Zakończenie wdrożenia zostanie potwierdzone protokołem podpisanym przez obie strony.

2.11 Podpisany obustronnie protokół zakończenia wdrożenia jest podstawą do wypłaty wynagrodzenia z tytułu zakupu i wdrożenia urządzenia UTM.

3. Licencjonowanie

3.1. Licencja do urządzenia zapewnia przez okres 5 lat:

a. aktualizacje do wszystkich modułów urządzenia (w tym do pasywnego skanera wnętrza sieci),
b. wsparcie techniczne od poniedziałku do piątku od 8.00 do 18.00,
c. wymianę urządzenia na nowe w przypadku awarii na następny dzień roboczy.

Informatyk
Sławomir Wujek

Główny Informatyk
Krzysztof Gut

BYTOMSKIE PRZEDSIĘBIORSTWO KOMUNALNE Sp. z o.o.
WICEPREZES ZARZĄDU ds. FINANSOWYCH
Jacek Matejczyk

BYTOMSKIE PRZEDSIĘBIORSTWO KOMUNALNE Sp.
PREZES ZARZĄDU
Dawid Zięba