Wymagania dla urządzenia UTM

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.
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.
System musi wspierać IPv4 oraz IPv6 w zakresie:

a. Firewall.
b. Ochrony w warstwie aplikacji.
c. Protokołów routingu dynamicznego.

Minimalne wymagania urządzenia:

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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45.
5. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
6. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 32 GB.
7. W zakresie Firewall'a obsługa nie mniej niż 1 mln jednoczesnych połączeń.
8. Przepustowość Firewall: nie mniej niż 2 Gbps.
9. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 400 Mbps.
10. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 800 Mbps lub wydajność skanowania ruchu w celu ochrony przed atakami w trybie „Enterprise Traffic Mix" o wartościach minimalnych: IPS min. 400 Mbps, NGFW min. 250 Mbps, Threat Protection min. 200 Mbps.
11. Musi obsługiwać co najmniej 50 mobilnych połączeń VPN.
12. Wsparcie VLAN: Musi posiadać minimum 50 sieci VLAN.
13. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
    b. Kontrola Aplikacji.
    c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
    e. Ochrona przed atakami - Intrusion Prevention System.

f. Kontrola stron WWW.
g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
h. Zarządzanie pasmem (QoS, Traffic shaping).
i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
k. Analiza ruchu szyfrowanego protokołem SSL.

14. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
15. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    a. Translację jeden do jeden oraz jeden do wielu.
    b. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
17. System musi umożliwiać konfigurację połączeń typu IPSec VPN.
18. System musi umożliwiać konfigurację połączeń typu SSL VPN.
19. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    a. Routingu statycznego.
    b. Policy Based Routingu.
20. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
21. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
22. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
23. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
24. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji.
25. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.
26. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
27. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
28. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
29. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
30. 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.
31. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
32. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
33. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
34. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

35. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
36. 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 avoidance.
37. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
38. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
39. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
40. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenie. Wykonawca jest odpowiedzialny za dostawę, instalację i konfigurację urządzenia zgodnie z wytycznymi Zamawiającego.
41. Gwarancja – min. 60 miesięcy gwarancji.