ZAŁĄCZNIK NR 1.11 do PFU

UTM i routery dostępowe w WN

1. UTM (Lokalizacja: GPD lub opcjonalnie BS01) – 1 szt.

Urządzenie lub zespół urządzeń klasy operatorskiej pełniące role routera brzegowego, swicha oraz systemu bezpieczeństwa, spełniające następujące wymogi:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Elementy wchodzące w skład systemu ochrony zostaną zrealizowane w postaci zamkniętej platformy sprzętowej.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
3. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent
4. System realizujący funkcję Firewall powinien dysponować minimum 16 interfejsami miedzianymi Ethernet 10/100/1000 oraz 2 portami SFP
5. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
6. W zakresie Firewall'a obsługa nie mniej niż 1,4mln jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.
7. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 16 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
8. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN

d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
e. Kontrola stron Internetowych – Web Filter [WF]
f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
g. Kontrola pasma oraz ruchu [QoS i Traffic shaping]
h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
i. Możliwość analizy ruchu szyfrowanego SSL'em oraz funkcja SSH proxy
j. Ochrona przed wyciekiem poufnej informacji (DLP)

9. Wydajność systemu Firewall min 2,5 Gbps
10. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 500 Mbps
11. Wydajność ochrony przed atakami (IPS) min 1,5 Gbps.
12. Wydajność IPSEC VPN, nie mniej niż 1,2 Gbps
13. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
    b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    d. Praca w topologii Hub and Spoke oraz Mesh
    e. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
    f. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    g. bsługa ssl vpn w trybach portal oraz tunel
14. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
16. Możliwość budowy min 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
17. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
18. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
19. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)

20. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 6000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
21. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
22. Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
23. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
24. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
25. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall powinien posiadać certyfikat ICSA dla rozwiązań kategorii Network Firewall
26. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

2. Router dostępowy - większe jednostki (Router Typ 1)

Urządzenie pełniące role routera dostępowego oraz systemu bezpieczeństwa, spełniające następujące wymogi:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowych. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy

wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. System realizujący funkcję Firewall powinien dawać możliwość pracy w trybach: routera z funkcją NAT lub mostu transparentnego.
2. System realizujący funkcję Firewall musi dysponować co najmniej 10 portami Ethernet, w tym min. 5 portami 10/100/1000 Base-TX i 1 interfejs SFP oraz min. 1 port USB umożliwiający podłączenie modemu GSM bezpośrednio lub przez adapter dostarczony wraz z urządzeniem
3. Nielimitowana możliwość tworzenia interfejsów wirtualnych VLAN w oparciu o standard 802.1Q.
4. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:
   a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection
   b. translacji adresów NAT i maskarada
   c. klasyfikacja ruchu i tworzenie reguł filtrowania minimum w oparciu o źródłowy adres MAC, źródłowy/docelowy adresu IP, źródłowy/docelowy port i zakres portów, protokół IP, zawartość pakietu, rozmiar pakietu,
   d. detekcja protokołu Warstwy 7
   e. zapewnienie poufności danych, obsługa VPN oraz protokołów IPSec i SSL VPN, sprzętowe wspomaganie szyfrowania
   f. możliwość realizacji ochrony przed atakami - Intrusion Prevention System [IPS/IDS]
   g. kontrola pasma oraz ruchu (QoS, Traffic shaping) w zakresie min:
      - ograniczenie prędkości i ustawienie priorytetów wg: adresu IP źródłowego i docelowego, protokołu, numeru portu, znacznika zapory sieciowej (firewall);
      - obsługa popularnych algorytmów RED, SFQ, PCQ, CIR, MIR;
      - ograniczenia wielkości kolejek PFIFO i BFIFO;
   h. wykrywanie ruchu P2P
5. Rozwiązanie powinno zapewniać wsparcie dla Policy Base Routing oraz obsługę routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP.
6. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania i autoryzowania użytkowników Hot-Spot, PPP, PPPoE, PPTP, L2TP za pomocą protokołu RADIUS
7. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTP, SSH, telnet, MAC telnet,) jak i współpracować z dedykowanym oprogramowaniem do zarządzania i monitorowania urządzeniami. Komunikacja oprogramowania z urządzeniami musi być realizowana z wykorzystaniem protokołu szyfrowanego.

8. Wbudowane narzędzia diagnostyczne: ping, traceroute, bandwith test, sniffer pakietów.
9. Możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.
10. Możliwość lokalnej i zdalnej aktualizacji oprogramowania.
11. Logowanie wszystkich połączeń przechodzące przez firewall oraz podjętych akcji (połączenia przepuszczone/odrzucone) na zewnętrzny serwer Syslog;
12. Bezpłatne aktualizacje oprogramowania urządzenia dostępne na stronie producenta.
13. Możliwość zasilania PoE.

3. Router dostępowy – małe jednostki w których podłączany jest tylko 1 komputer (Router Typ 2)

Urządzenie pełniące role routera dostępowego oraz systemu bezpieczeństwa, spełniające następujące wymogi:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowych. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. System realizujący funkcję Firewall powinien dawać możliwość pracy w trybach: routera z funkcją NAT lub mostu transparentnego.
2. Co najmniej 5 portów 10/100Base-TX
3. Nielimitowana możliwość tworzenia interfejsów wirtualnych VLAN w oparciu o standard 802.1Q.
4. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:
   a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection
   b. translacji adresów NAT i maskarada
   c. klasyfikacja ruchu i tworzenie reguł filtrowania minimum w oparciu o źródłowy adres MAC, źródłowy/docelowy adresu IP, źródłowy/docelowy port i zakres portów, protokół IP, zawartość pakietu, rozmiar pakietu,
   d. detekcja protokołu Warstwy 7
   e. zapewnienie poufności danych, obsługa VPN oraz protokołów IPSec i SSL VPN, sprzętowe wspomaganie szyfrowania

f. kontrola pasma oraz ruchu (QoS, Traffic shaping) w zakresie min:
   - ograniczenie prędkości i ustawienie priorytetów wg: adresu IP źródłowego i docelowego, protokołu, numeru portu, znacznika zapory sieciowej (firewall);
   - obsługa popularnych algorytmów RED, SFQ, PCQ, CIR, MIR;
   - ograniczenia wielkości kolejek PFIFO i BFIFO;

g. wykrywanie ruchu P2P

5. Rozwiązanie powinno zapewniać obsługę routingu statycznego i dynamicznego.
6. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania i autoryzowania użytkowników Hot-Spot, PPP, PPPoE, PPTP, L2TP za pomocą protokołu RADIUS
7. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTP, SSH, telnet, MAC telnet) jak i współpracować z dedykowanym oprogramowaniem do zarządzania i monitorowania urządzeniami. Komunikacja oprogramowania z urządzeniami musi być realizowana z wykorzystaniem protokołu szyfrowanego.
8. Wbudowane narzędzia diagnostyczne: ping, traceroute, bandwith test, sniffer pakietów.
9. Możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.
10. Możliwość lokalnej i zdalnej aktualizacji oprogramowania.
11. Logowanie wszystkich połączeń przechodzące przez firewall oraz podjętych akcji (połączenia przepuszczone/odrzucone) na zewnętrzny serwer Syslog;
12. Bezpłatne aktualizacje oprogramowania urządzenia dostępne na stronie producenta.
13. Możliwość zasilania PoE.