**Nasz znak: 34/DU/Z/13 Data 20.02.2014 r.**

### KOMUNIKAT nr 11

**do postępowania nr 34/DU/Z/13**

Zamawiający informuje, że w prowadzonym postępowaniu nr 34/DU/Z/13 zmianie ulegają zapisy SIWZ w załączniku nr 7 oraz załączniku nr 9 w następujących punktach:

**Zmiana nr 1**

#### 9.1.3.4 „Wymagania szczegółowe dla stosowanych produktów – firewalle wewnętrzne” w wymaganiu dla FWW.NET.CG oraz FWW.NET.CZ usuwa się treść zaznaczoną na czerwono:

Było:

Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własny procesor. Karty usługowe muszą realizować sprzętowo co najmniej takie funkcje jak stateful firewall, IPSec VPN, intrusion prevention (IPS). Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Urządzenie musi posiadać minimum 8 uniwersalnych slotów pozwalających na zainstalowanie i uruchomienie minimum 4 karty serwisowe.

Jest:

Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własny procesor. Karty usługowe muszą realizować sprzętowo co najmniej takie funkcje jak stateful firewall, IPSec VPN. Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Urządzenie musi posiadać minimum 8 uniwersalnych slotów pozwalających na zainstalowanie i uruchomienie minimum 4 karty serwisowe.

Jednocześnie usuwa się zapis:

Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) realizowaną na modułach usługowych. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące DDoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Urządzenie musi realizować zadania IPS z wydajnością nie mniejszą niż 4 Gb/s w trybie inline (wydajność w pełni niezależna od funkcjonalności opisanych w pkt 7 i 9). Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta minimum jeden raz w tygodniu. Funkcjonalność IPS musi być realizowana przez dedykowane karty usługowe

**Zmiana nr 2**

#### 9.1.8.3 „Wymagania szczegółowe dla stosowanych produktów – stacja zarządzająca” w wymaganiu dla stacji zarządzającej MGM.NET usuwa się treść zaznaczoną na czerwono:

Było:

1. Zdalne zarządzanie i zdalna konfiguracja Urządzeń – tj. przełączników (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]) oraz routerów (RTR.NET.CG, RTR.NET.CZ)
2. Możliwość tworzenia wielu użytkowników o różnym poziomie uprawnień do zarządzania różnymi grupami urządzeń (RBAC: Role Based Access Control).
3. Elastyczne metody uwierzytelnienia użytkowników systemu: lokalnie lub przez usługi AAA: LDAP, RADIUS oraz TACACS+
4. Zapis wybranych przez użytkowników zdarzeń typu SNMP trap i syslog,
5. Oprogramowanie do zarządzania urządzeniami sieci LAN musi stanowić zintegrowany pakiet aplikacji do konfiguracji, administracji, monitoringu i diagnozowania sieci.
6. Musi umożliwiać zarządzanie dostarczanymi urządzeniami, w tym firewall z IDS/IPS.
7. Wymagany ogólny zakres funkcjonalności:
   1. Wykrywanie błędów i problemów w czasie rzeczywistym,
   2. Wykrywanie urządzeń końcowych i wolnych portów,
   3. Narzędzia do zarządzania listą urządzeń (ang. inventory management), oprogramowaniem urządzeń i ich konfiguracją, w tym umożliwiające tworzenie archiwów konfiguracji dla poszczególnych urządzeń,
   4. Diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,
   5. Generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji.
8. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie urządzeniami firewall w zakresie:
   1. Zarządzania firewallami działającymi na poziomie L3,
   2. Zarządzania funkcjami firewalli aplikacyjnych,
   3. Definiowanie reguł polityki bezpieczeństwa
   4. Definiowanie reguł translacji NAT
   5. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,
   6. Konfiguracji rutingu na zarządzanych urządzeniach,
   7. Definiowania i konfiguracji usług sieciowych,
   8. Konfiguracji, zarządzania i monitoringu funkcjonalności failover,
   9. Tworzenia sieci VPN z wykorzystaniem kreatorów,
   10. Monitoringu sieci VPN.
9. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie urządzeniami IDS/IPS w zakresie:
   1. Zarządzania sygnaturami, w tym ich przeglądania, aktywacji/ dezaktywacji, kopiowania i modyfikacji,
   2. Przeglądu i tworzenia polityk IDS/IPS,
   3. Tworzenia sygnatur IDS/IPS,
   4. Automatycznego uaktualniania oprogramowania sond,
   5. Monitoringu stanu pracy urządzeń.
10. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie przełącznikami   
    w zakresie:
    1. Zarządzania protokołami rutingu,
    2. Zarządzania sieciami wirtualnymi (VLAN),
    3. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,
    4. Konfiguracji portów urządzenia z wykorzystaniem predefiniowanych profili,
    5. Zarządzania rodziną protokołów STP a także zabezpieczania działania STP z wykorzystaniem mechanizmów Root Guard, BPDU Guard, edge port,
    6. Konfiguracja ustawień dotyczących bezpieczeństwa portu ang. port security, co najmniej w zakresie limitowania adresów MAC, ARP inspection, DHCP snooping,
    7. Zarządzania listami kontroli dostępu.
11. Pełna obsługa systemów logicznych (np. stacki przełączników, grupowanie przełączników w jeden przełącznik wirtualny
12. Stacja zarządzająca może zostać dostarczona w postaci urządzenia appliance lub oprogramowania instalowanego na serwerze ogólnego przeznaczenia. W przypadku oprogramowania należy dostarczyć system operacyjny oraz serwer zgodny z wymaganiami stawianymi przez producenta oprogramowania zarządzającego
13. System zarządzania musi pochodzić z oferty producenta oferowanych przełączników i routerów.
14. System zarządzania musi posiadać licencje potrzebne do zarządzania wszystkimi Urządzeniami - tj przełącznikami (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]), routerami (RTR.NET.CG, RTR.NET.CZ), bramkami SSLVPN – (SSL.NET.CG, SSL.NET.CZ) oraz Firewallami wewnętrznymi (FWW.NET.CG, FWW.NET.CZ)

Jest:

1. Zdalne zarządzanie i zdalna konfiguracja Urządzeń - tj przełączników (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]) oraz routerów (RTR.NET.CG, RTR.NET.CZ)
2. Możliwość tworzenia wielu użytkowników o różnym poziomie uprawnień do zarządzania różnymi grupami urządzeń (RBAC: Role Based Access Control).
3. Elastyczne metody uwierzytelnienia użytkowników systemu: lokalnie lub przez usługi AAA: LDAP, RADIUS oraz TACACS+
4. Zapis wybranych przez użytkowników zdarzeń typu SNMP trap i syslog,
5. Oprogramowanie do zarządzania urządzeniami sieci LAN musi stanowić zintegrowany pakiet aplikacji do konfiguracji, administracji, monitoringu i diagnozowania sieci.
6. Musi umożliwiać zarządzanie dostarczanymi urządzeniami, w tym firewall.
7. Wymagany ogólny zakres funkcjonalności:
   1. Wykrywanie błędów i problemów w czasie rzeczywistym,
   2. Wykrywanie urządzeń końcowych i wolnych portów,
   3. Narzędzia do zarządzania listą urządzeń (ang. inventory management), oprogramowaniem urządzeń i ich konfiguracją, w tym umożliwiające tworzenie archiwów konfiguracji dla poszczególnych urządzeń,
   4. Diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,
   5. Generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji.
8. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie urządzeniami firewall w zakresie:
   1. Zarządzania firewallami działającymi na poziomie L3,
   2. Zarządzania funkcjami firewalli aplikacyjnych,
   3. Definiowanie reguł polityki bezpieczeństwa
   4. Definiowanie reguł translacji NAT
   5. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,
   6. Konfiguracji rutingu na zarządzanych urządzeniach,
   7. Definiowania i konfiguracji usług sieciowych,
   8. Konfiguracji, zarządzania i monitoringu funkcjonalności failover,
   9. Tworzenia sieci VPN z wykorzystaniem kreatorów,
   10. Monitoringu sieci VPN.
   11. Monitoringu stanu pracy urządzeń.
9. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie przełącznikami   
   w zakresie:
   1. Zarządzania protokołami rutingu,
   2. Zarządzania sieciami wirtualnymi (VLAN),
   3. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,
   4. Konfiguracji portów urządzenia z wykorzystaniem predefiniowanych profili,
   5. Zarządzania rodziną protokołów STP a także zabezpieczania działania STP z wykorzystaniem mechanizmów Root Guard, BPDU Guard, edge port,
   6. Konfiguracja ustawień dotyczących bezpieczeństwa portu ang. port security, co najmniej w zakresie limitowania adresów MAC, ARP inspection, DHCP snooping,
   7. Zarządzania listami kontroli dostępu.
10. Pełna obsługa systemów logicznych (np. stacki przełączników, grupowanie przełączników w jeden przełącznik wirtualny
11. Stacja zarządzająca może zostać dostarczona w postaci urządzenia appliance lub oprogramowania instalowanego na serwerze ogólnego przeznaczenia. W przypadku oprogramowania należy dostarczyć system operacyjny oraz serwer zgodny z wymaganiami stawianymi przez producenta oprogramowania zarządzającego
12. System zarządzania musi pochodzić z oferty producenta oferowanych przełączników i routerów.
13. System zarządzania musi posiadać licencje potrzebne do zarządzania wszystkimi Urządzeniami - tj przełącznikami (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]), routerami (RTR.NET.CG, RTR.NET.CZ), bramkami SSLVPN – (SSL.NET.CG, SSL.NET.CZ) oraz Firewallami wewnętrznymi (FWW.NET.CG, FWW.NET.CZ)

**Zmiana nr 3**

**Dotyczy tylko załącznika nr 9 do SIWZ**

9.1.11.2 Zakres dokumentacji powykonawczej w ust. 4 pkt. c ppkt. V usuwa się treść zaznaczoną na czerwono:

Było:

Ust. 4 pkt. c - Firewalle Wewnętrzne (FWW.NET.CG oraz FWW.NET.CZ)

* + 1. Konfiguracja reguł routingu
    2. Konfiguracja przepływów ruchu sieciowego z określeniem stref bezpieczeństwa, wykorzystywanych aplikacji i kierunków komunikacji
    3. Konfiguracja polityki bezpieczeństwa uwzględniającej reguły zapór sieciowych, reguły translacji adresów i reguły szyfrowania
    4. Konfiguracja polityki dostępu do chronionych sieci VLAN dla pracowników i studentów
    5. Konfiguracja polityki ochrony przed intruzami (IPS), system dla chronionych sieci VLAN
    6. Konfiguracja mechanizmów „disaster recovery”

Jest:

Ust. 4 pkt. c - Firewalle Wewnętrzne (FWW.NET.CG oraz FWW.NET.CZ)

1. Konfiguracja reguł routingu
2. Konfiguracja przepływów ruchu sieciowego z określeniem stref bezpieczeństwa, wykorzystywanych aplikacji i kierunków komunikacji
3. Konfiguracja polityki bezpieczeństwa uwzględniającej reguły zapór sieciowych, reguły translacji adresów i reguły szyfrowania
4. Konfiguracja polityki dostępu do chronionych sieci VLAN dla pracowników i studentów
5. Konfiguracja mechanizmów „disaster recovery”

**W związku z powyższym Zamawiający podjął decyzję o przedłużeniu terminu składania ofert z określonego na dzień 24.02.2014 r. godz. 12:00 na nowy wyznaczony na dzień 17.03.2014 r. godz. 12:00.**

**Zmianie ulega również termin otwarcia ofert z 24.02.2014 godz. 12:15 na 17.03.2014 r. godz. 12:15.**

**Miejsce składania i otwarcia ofert pozostaje bez zmian.**

**Jednocześnie informujemy, że przesunięciu ulegają odpowiednio także inne terminy: początek biegu terminu związania ofert oraz termin dotyczący wpłacania wadium.**

**Zwracamy uwagę na uwzględnienie powyższej zmiany terminu składania ofert przy ustaleniu terminu ważności wadium składanych w formie dokumentu (np. gwarancji bankowej lub ubezpieczeniowej).**