warunki świadczenia usługi IP VPN Protected

Rozdział 1

Terminologia stosowana w Warunkach świadczenia usługi IP VPN Protected

§ 1

1. Użyte w Warunkach świadczenia usługi IP VPN Protected pojęcia oznaczają:
   1) **Cisco ISR (ang. Integrated Service Router)** – rutery wykorzystywane jako Rutery CE w usłudze IP VPN oraz wykorzystywane do świadczenia usługi IP VPN Protected.
   2) **Cisco MARS (ang. Monitoring, Analysis And Response System)** – urządzenie, wraz odpowiednim oprogramowaniem, służące do zbierania informacji, monitorowania i śledzenia zdarzeń na Ruterach CE.
   3) **Dostęp do Internetu** - dostęp do sieci publicznej Internet.
   4) **Firewall** – oprogramowanie i/lub sprzęt zlokalizowany pomiędzy sieciami telekomunikacyjnymi, uniemożliwiający dostęp nieautoryzowanym użytkownikom do sieci LAN Abonenta.
   5) **IPS (ang. Intrusion Prevention System)** – oprogramowanie i/lub sprzęt pozwalające na inspekcję ruchu przychodzącego do lokalizacji Abonenta jak i ruchu wychodzącego z jego lokalizacji, realizowaną przy pomocy sygnatur służących do wyszukiwania określonych wzorów w transmitowanych danych, wykrywające zagrożenia i blokujące przed ich dotarciem do zasobów informatycznych Abonenta.
   6) **IOS (ang. Internetwork Operating System)** – system operacyjny dedykowany Cisco ISR.
   7) **Usługa IP VPN Protected** – usługi dodatkowe dla usługi IP VPN.
   8) **IP VPN Protected Firewall** – opcja Usługi IP VPN Protected, implementowana na Cisco ISR w systemie operacyjnym IOS, zapobiegająca przenikaniu do sieci LAN Abonenta niepożądanych informacji i zjawisk pochodzących z sieci Internet.
   9) **IP VPN Protected IPS (ang. Instrusion Prevention System)** – opcja Usługi IP VPN Protected umożliwiająca blokowanie dostępu intruzów, rozpoznająca i blokująca zagrożenia w sieci Abonenta, w tym robaki, wirusy, spyware, adware oraz niewłaściwe wykorzystanie oprogramowania. Opcja jest implementowana na Cisco ISR w systemie operacyjnym IOS.
   10) **IP VPN Protected Raportowanie** – opcja Usługi IP VPN Protected pozwalająca na monitorowanie i śledzenie akcji oraz incydentów związanych z bezpieczeństwem Ruterów CE.
   11) **IP VPN Protected Szyfrowanie** - opcja Usługi IP VPN Protected pozwalająca na szyfrowanie ruchu protokołami IP Sec.
   12) **Sygnatury IPS** - reguły definiujące typowy niebezpieczny ruch w sieci dostarczane TP przez Cisco.
   13) **Specyfikacja usługi IP VPN Protected** – załącznik do „Umowy o świadczenie przez Telekomunikację Polską S.A. usługi IP VPN oraz usługi IP VPN Protected dla usługi IP VPN",

określający lokalizacje i opcje Usługi IP VPN Protected oraz terminy uruchomienia usługi w poszczególnych lokalizacjach.

14) **Szyfrowanie** – szyfrowanie pakietów z wykorzystaniem mechanizmów kryptograficznych.

2. Pojęcia użyte w Warunkach świadczenia usługi IP VPN Protected, rozpoczynające się od wielkiej litery i nie zdefiniowane w ust. 1, są używane w znaczeniu przyjętym w Regulaminie usługi IP VPN.

Rozdział 2

Postanowienia ogólne

§ 2

1. Usługa IP VPN Protected jest realizowana na podstawie Warunków świadczenia usługi IP VPN Protected oraz Regulaminu usługi IP VPN.
2. Uruchomienie Usługi IP VPN Protected następuje w terminach wskazanych w Specyfikacji usługi IP VPN Protected.
3. Przekazanie Urządzeń następuje na podstawie protokołów zdawczo-odbiorczych usługi IP VPN.
4. Wysokość opłat za Usługę IP VPN Protected określa Specyfikacja cenowa.
5. W sprawach nieuregulowanych w niniejszym dokumencie stosuje się odpowiednio Regulamin usługi IP VPN.

Rozdział 3

Zakres i warunki świadczenia usługi IP VPN Protected

§ 3

1. W ramach Usługi IP VPN Protected TP świadczy następujące opcje:
   1) IP VPN Protected Firewall,
   2) IP VPN Protected IPS,
   3) IP VPN Protected Szyfrowanie,
   4) IP VPN Protected Monitorowanie i raportowanie.
2. Świadczenie Usługi IP VPN Protected odbywa się z wyłącznie z wykorzystaniem Cisco ISR i/lub Cisco MARS.
3. TP może świadczyć na wniosek Abonenta każdą z opcji Usługi IP VPN Protected, z zastrzeżeniem § 5 ust. 1.

§ 4

1. IP VPN Protected Firewall jest świadczona w danej lokalizacji w jednym z trzech wariantów wybranych przez Abonenta:
   1) bez zdefiniowanej polityki dostępu do sieci LAN Abonenta:
      a) brak dostępu do Internetu – Intranet, sieć IP VPN Abonenta bez dostępu do Internetu,
      b) z dostępem do Internetu – blokowany jest ruch inicjowany i pochodzący z innych adresów źródłowych w tym z Internetu,
   2) ze standardową polityką działania Firewall, tzn. ruch z siedziby Abonenta nie jest zatrzymywany, a ruch inicjowany z zewnątrz jest zatrzymywany, z jednoczesną blokadą ruchu z Internetu oraz otwarciem ruchu do Internetu,
   3) ze zdefiniowaną polityką przez Abonenta przy pomocy odpowiedniego formularza w formacie .xls.
2. IP VPN Protected Firewall pozwala na wykorzystanie funkcjonalności Firewall implementowanej na ruterach Cisco ISR. Funkcjonalność Firewall obejmuje:

1) zapewnienie dostępu do sieci Abonenta ruchu tylko autoryzowanego,

2) umożliwienie filtracji ruchu (ang. stateful inspection),

3) kontrole działania aplikacji (ang. aplication inspection),

4) umożliwienie inspekcji pakietów,

5) zapewnienie separacji między siecią VPN Abonenta a Internetem.

3. Zmiany konfiguracji IP VPN Protected Firewall wykonywane są na wniosek Abonenta zgodnie z zasadami obowiązującymi dla zmian konfiguracji usługi IP VPN.

4. TP pobiera jednorazowe opłaty za zmianę konfiguracji usługi IP VPN Protected Firewall, przy czym dokonanie przez Abonenta jednokrotnej zmiany konfiguracji raz w miesiącu jest nieodpłatne. Każda następna zmiana jest odpłatna, a jej wysokość odpowiada opłacie za zmianę konfiguracji usługi IP VPN.

§ 5

1. IP VPN Protected IPS wykorzystuje funkcjonalność IPS implementowaną na Cisco ISR, która:

   1) umożliwia przeprowadzanie inspekcji pakietów wchodzących i wychodzących,

   2) umożliwia wykrywanie i blokowanie ruchu zidentyfikowanego jako złośliwy,

   3) wykorzystuje system sygnatur do przeprowadzenia inspekcji ruchu.

2. IP VPN Protected IPS jest definiowana przy pomocy odpowiednich sygnatur implementowanych przez TP na Cisco ISR.

3. Uruchomienie IP VPN Protected IPS następuje po pierwszej implementacji listy sygnatur na Cisco ISR. Kolejne aktualizacje sygnatur będą odbywały się automatycznie.

4. W ramach Usługi IP VPN Protected IPS jedna lista sygnatur implementowana jest dla całej sieci Abonenta.

5. Uaktualnienie sygnatur (dodanie nowych sygnatur) odbywać się będzie automatycznie w każdy poniedziałek w godzinach 06.00-06.30.

6. Po każdym uaktualnieniu sygnatur Abonent może zgłosić wniosek o wyłączenie nowo dodanej sygnatury. Realizacja zgłoszonego wniosku jest bezpłatna. Włączenie wcześniej wyłączonej sygnatury będzie realizowane jak nieodpłatna zmiana konfiguracji Cisco ISR i nie jest wliczana do ilości bezpłatnych zmian konfiguracji Rutera CE.

7. W przypadku wystąpienia kolizji zaimplementowanej sygnatury z polityką ruchu Abonenta, powinien on zgłosić ten fakt do TP. W takim przypadku TP dokona wyłączenia sygnatury, w trybie zmiany konfiguracji usługi IP VPN.

§ 6

1. Z opcji IP VPN Protected Raportowanie może korzystać Abonent, który posiada usługę IP VPN Protected Firewall lub IP VPN Protected IPS.

2. IP VPN Protected Raportowanie realizuje następujące zadania:

   1) zbiera informacje z Cisco ISR o odnotowanych zdarzeniach w sieci Abonenta,

   2) przedstawia próby wprowadzania do sieci szkodliwych aplikacji,

   3) przedstawia zmiany w zdefiniowanej przez Abonenta polityce bezpieczeństwa IP VPN Protected Firewall oraz IP VPN Protected IPS,

   4) monitoruje i raportuje zdarzenia w sieci Abonenta.

3. Uruchomienie IP VPN Protected Raportowanie odbywa się po zainstalowaniu sprzętu oraz odpowiednim skonfigurowaniu oprogramowania.

4. Abonent otrzymuje interfejs graficzny Cisco MARS w trybie tylko do odczytu (bez możliwości wykonywania zmian).
5. Instalacja Cisco MARS odbywa się w lokalizacji wskazanej przez Abonenta.
6. Cisco MARS w IP VPN Protected Raportowanie nie podejmuje reakcji na występujące zdarzenia w sieci Abonenta.

Rozdział 4

Odpowiedzialność

§ 7

1. W przypadku świadczenia Usługi IP VPN Protected TP nie ponosi odpowiedzialności za pełne bezpieczeństwo sieci telekomunikacyjnej Abonenta.
2. Dla Usługi IP VPN Protected TP zapewnia obsługę serwisową na zasadach określonych w Regulaminie usługi IP VPN.