

IBM

@server

iSeries

Wirtualne sieci prywatne

*Wersja 5 wydanie 3*







@server

iSeries

Wirtualne sieci prywatne

*Wersja 5 wydanie 3*

**Uwaga**

Przed korzystaniem z niniejszych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w dodatku "Uwagi", na stronie 69.

**Wydanie szóste (sierpień 2005)**

To wydanie dotyczy wersji 5, wydania 3, modyfikacji 2 systemu IBM i5/OS (5722-SS1) i wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zaznaczono inaczej. Wersja ta nie działa na wszystkich modelach komputerów o zredukowanej liczbie instrukcji (RISC) ani na modelach komputerów CISC.

© Copyright International Business Machines Corporation 1998, 2005. Wszelkie prawa zastrzeżone.

# Spis treści

## Wirtualne sieci prywatne . . . . . 1

Co nowego w wersji V5R3 . . . . .	2
Drukowanie tego dokumentu . . . . .	3
Scenariusze dla sieci VPN . . . . .	3
Scenariusz VPN: Podstawowe połączenie z biurem oddziału . . . . .	4
Szczegóły konfigurowania . . . . .	6
Scenariusz VPN: Podstawowe połączenie pomiędzy firmami . . . . .	8
Szczegóły konfigurowania . . . . .	10
Scenariusz VPN: Ochrona dobrowolnego tunelu L2TP za pomocą protokołu IPSec . . . . .	13
Szczegóły konfigurowania . . . . .	15
Scenariusz VPN: Wykorzystanie translacji adresów sieciowych na potrzeby sieci VPN . . . . .	19
Koncepcje sieci VPN . . . . .	21
Protokoły IP Security (IPSec) . . . . .	21
Protokół Authentication Header . . . . .	22
Protokół Encapsulating Security Payload . . . . .	23
Kombinacja protokołów AH i ESP . . . . .	24
Zarządzanie kluczami . . . . .	24
Protokół Layer 2 Tunnel Protocol (L2TP) . . . . .	26
Translacja adresów sieciowych dla sieci VPN . . . . .	26
Zgodność translacji NAT i protokołów IPSec . . . . .	27
Protokół IP Compression (IPComp) . . . . .	29
Sieci VPN i filtrowanie IP . . . . .	29
Migracja filtrów strategii do bieżącej wersji systemu . . . . .	29
Połączenie VPN bez filtrów strategii . . . . .	30
Niejawne zezwolenie na ruch danych IKE . . . . .	31
Planowanie sieci VPN . . . . .	31
Wymagania konfiguracyjne VPN . . . . .	31
Określenie typu tworzonej sieci VPN . . . . .	32
Arkusze planowania VPN . . . . .	33
Arkusze planowania dla połączeń dynamicznych . . . . .	33
Arkusze planowania dla połączeń ręcznych . . . . .	34
Konfigurowanie połączeń VPN . . . . .	36
Konfigurowanie połączeń za pomocą Kreatora nowego połączenia . . . . .	38
Konfigurowanie strategii ochrony VPN . . . . .	38
Konfigurowanie strategii protokołu Internet Key Exchange (IKE) . . . . .	38
Konfigurowanie strategii danych . . . . .	39
Konfigurowanie chronionego połączenia VPN . . . . .	39
Konfigurowanie połączeń ręcznych . . . . .	40
Konfigurowanie reguł pakietów VPN . . . . .	40
Konfigurowanie reguły filtrowania typu Pre-IPSec . . . . .	41
Konfigurowanie reguły filtrowania strategii . . . . .	42
Definiowanie interfejsu dla reguły filtrowania VPN . . . . .	43
Uaktywnianie reguł pakietów VPN . . . . .	44
Uruchamianie połączenia VPN . . . . .	44
Zarządzanie połączeniami VPN . . . . .	44
Ustawianie domyślnych atrybutów połączeń . . . . .	45
Resetowanie połączeń w wypadku wystąpienia błędu . . . . .	45
Wyświetlanie informacji o błędach . . . . .	45
Wyświetlanie atrybutów połączeń aktywnych . . . . .	46

Korzystanie z programu do śledzenia serwera VPN . . . . .	46
Wyświetlanie protokołów zadań serwera VPN . . . . .	46
Wyświetlanie atrybutów powiązań Security Association (SA) . . . . .	47
Zatrzymywanie połączeń VPN . . . . .	47
Usuwanie obiektów konfiguracyjnych VPN . . . . .	47
Rozwiązywanie problemów dotyczących połączeń VPN . . . . .	47
Wprowadzenie do rozwiązywania problemów dotyczących połączeń VPN . . . . .	48
Typowe błędy konfiguracyjne i sposoby ich usuwania . . . . .	49
Komunikat o błędzie połączenia VPN: TCP5B28 . . . . .	50
Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji . . . . .	50
Komunikat o błędzie połączenia VPN: NIEPOPRAWNY PARAMETR PINBUF . . . . .	51
Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji, Zdalny serwer kluczy... . . . . .	51
Komunikat o błędzie połączenia VPN: Nie można zaktualizować obiektu . . . . .	52
Komunikat o błędzie połączenia VPN: Nie można zaszyfrować klucza... . . . . .	52
Komunikat o błędzie połączenia VPN: CPF9821 . . . . .	53
Błąd połączenia VPN: Wszystkie klucze są puste . . . . .	53
Błąd połączenia VPN: Wyświetlenie ekranu wpisania się do innego systemu podczas korzystania z Edytora reguł pakietów . . . . .	53
Błąd połączenia VPN: Pusty status połączenia w oknie programu iSeries Navigator . . . . .	53
Błąd połączenia VPN: Po zatrzymaniu połączenie ma status Włączone . . . . .	53
Błąd połączenia VPN: Nie można wybrać algorytmu szyfrowania 3DES . . . . .	54
Błąd połączenia VPN: W oknie programu iSeries Navigator wyświetlane są nieoczekiwane kolumny . . . . .	54
Błąd połączenia VPN: Nie można dezaktywować aktywnych reguł filtrowania . . . . .	54
Błąd połączenia VPN: Zmiana grupy z kluczem dynamicznym dla połączenia . . . . .	54
Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QIPFILTER . . . . .	54
Pola kroniki QIPFILTER . . . . .	56
Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QVPN . . . . .	57
Pola kroniki QVPN . . . . .	58
Rozwiązywanie problemów dotyczących połączeń VPN za pomocą protokołów zadań VPN . . . . .	59
Często spotykane komunikaty o błędach Menedżera połączeń VPN . . . . .	60
Rozwiązywanie problemów dotyczących połączeń VPN za pomocą śledzenia komunikacji w systemie OS/400 . . . . .	65
Informacje pokrewne dla sieci VPN . . . . .	67

## Dodatek. Uwagi . . . . . 69

Znaki towarowe . . . . .	70
Warunki pobierania i drukowania publikacji . . . . .	71



---

## Wirtualne sieci prywatne

Sieć VPN (virtual private network) umożliwia firmie bezpieczne rozszerzenie prywatnego intranetu za pomocą istniejącej struktury sieci publicznej, na przykład Internetu. Dzięki VPN firma może sterować ruchem w sieci przy jednoczesnym zapewnieniu ważnych opcji zabezpieczających, takich jak uwierzytelnianie i ochrona danych.

Produkt OS/400<sup>(R)</sup> VPN to instalowany opcjonalnie komponent programu iSeries<sup>(TM)</sup> Navigator, graficznego interfejsu użytkownika systemu OS/400. Pozwala on tworzyć zabezpieczone na całej długości ścieżki połączeń pomiędzy dowolnymi hostami i bramami. Komponent OS/400 VPN wykorzystuje metody uwierzytelniania, algorytmy szyfrujące i inne mechanizmy ochronne, w celu zapewnienia bezpieczeństwa danych przesyłanych pomiędzy dwoma punktami końcowymi połączenia.

Połączenia VPN działają w warstwie sieci warstwowego modelu stosu komunikacyjnego TCP/IP. W szczególności wykorzystują one otwartą strukturę architektury IP Security Architecture (IPSec). Protokół IPSec udostępnia podstawowe funkcje ochrony dla Internetu, a także dostarcza elastyczne elementy konstrukcyjne, z których można budować odporne, bezpieczne wirtualne sieci prywatne.

Sieci VPN obsługują również rozwiązania z protokołem L2TP (Layer 2 Tunnel Protocol). Połączenia L2TP, zwane również liniami wirtualnymi, oferują zdalnym użytkownikom ekonomiczną metodę dostępu, umożliwiając serwerom sieci korporacyjnych obsługę adresów IP przypisanych tym użytkownikom. Ponadto połączenia L2TP zapewniają bezpieczny dostęp do systemów i sieci chronionych przez protokół IPSec.

Istotne jest zrozumienie wpływu, jaki połączenia VPN będą wywierały na całą sieć. Kluczowe czynniki powodzenia w tym względzie to odpowiedni plan i strategia implementacji. Aby dowiedzieć się, jak działają sieci VPN i jak się nimi posługiwać, warto przeczytać następujące sekcje:

### **“Co nowego w wersji V5R3” na stronie 2**

W sekcji przedstawiono zagadnienia nowe lub znacznie zmienione w tym wydaniu.

### **“Drukowanie tego dokumentu” na stronie 3**

Sekcja przeznaczona dla tych użytkowników, którzy preferują czytanie drukowanej wersji tego dokumentu; zawiera informacje dotyczące drukowania pliku PDF.

### **“Scenariusze dla sieci VPN” na stronie 3**

Aby poznać podstawowe typy sieci VPN i czynności związane z ich konfigurowaniem, należy przeczytać scenariusze przedstawione w tej sekcji.

### **“Konceptje sieci VPN” na stronie 21**

Użytkownik powinien mieć co najmniej podstawową wiedzę na temat standardowych technologii VPN. W tej sekcji przedstawiono ogólne informacje o protokołach używanych w implementacji sieci VPN.

### **“Planowanie sieci VPN” na stronie 31**

Pierwszym krokiem ku pomyślnemu wdrożeniu sieci VPN jest planowanie. W tej sekcji przedstawiono informacje dotyczące migracji ze starszych wersji, wymagania instalacyjne oraz odsyłacze do doradcy w zakresie planowania, który wygeneruje arkusz planowania dostosowany do konkretnych specyfikacji.

### **“Konfigurowanie połączeń VPN” na stronie 36**

Po zaplanowaniu sieci VPN można zacząć je konfigurować. Ta sekcja zawiera przegląd możliwości i metod wykorzystania sieci VPN.

### **“Zarządzanie połączeniami VPN” na stronie 44**

W sekcji opisano różne zadania związane z zarządzaniem aktywnymi połączeniami VPN, w tym zmianę tych połączeń, ich monitorowanie i usuwanie.

## “Rozwiązywanie problemów dotyczących połączeń VPN” na stronie 47

Z treścią tej sekcji należy się zapoznać w razie pojawienia się trudności z połączeniami VPN.

## “Informacje pokrewne dla sieci VPN” na stronie 67

Zbiór odsyłaczy do innych źródeł informacji o sieciach VPN i tematach pokrewnych.

---

## Co nowego w wersji V5R3

### Rozszerzenia funkcji

Wprowadzone w wersji 5 wydanie 3 (V5R3) rozszerzenia dotyczące funkcji wirtualnych sieci prywatnych (VPN) obejmują dwa nowe typy identyfikatorów. Są to dwa nowe typy identyfikatorów, które można wybrać podczas definiowania strategii wymiany kluczy i punktów końcowych danych połączenia VPN. Typy identyfikatorów obejmują lokalny adres IP i nazwę hosta protokołu IPv4. Dodatkowe informacje zawiera pomoc elektroniczna programu iSeries<sup>(TM)</sup> Navigator.

- **Mój lokalny adres IP**

Ten typ identyfikatora można wybrać, aby zdefiniować lokalny serwer kluczy dla strategii protokołu Internet Key Exchange lub lokalny punkt końcowy danych w definicji połączenia. Gdy zostanie on wybrany, połączenie VPN użyje dostępnego adresu IPv4. Połączenia VPN, które używają tego typu identyfikatora, nie mogą używać filtra strategii. Ponadto system lokalny musi być inicjatorem połączenia.

- **Nazwa hosta protokołu IPv4**

Ten typ identyfikatora można wybrać, aby zdefiniować kilka różnych parametrów:

- Zdalny serwer kluczy w strategii protokołu Internet Key Exchange.
- Identyfikator adresu zdalnego we właściwościach połączenia.
- Definicja filtra strategii dla właściwości grupy połączeń.

Nazwa hosta protokołu IPv4 tłumaczona na adres IP hosta podanego jako typ identyfikatora.

### Uwagi związane z bezpieczeństwem sieci VPN:

Zaleca się używanie trybu głównego uzgadniania zawsze wtedy, gdy do uwierzytelniania używany jest wstępny klucz współużytkowany. Zapewnia on bardziej bezpieczną wymianę. Jeśli konieczne jest użycie wstępnych kluczy współużytkowanych i agresywnego trybu negocjacji, należy wybrać trudne słowa, których nie można złamać podczas przeszukiwania słownika pod kątem możliwych haseł. Instrukcje dotyczące wymuszania wymiany kluczy z uzgadnianiem trybu głównego zawiera sekcja Ryzyko naruszenia ochrony przy uwierzytelnieniu z użyciem wstępnego klucza współużytkowanego. Podczas tworzenia lub edycji strategii protokołu Internet Key Exchange można użyć również pomocy elektronicznej programu iSeries Navigator, w której zamieszczone zostały bardziej szczegółowe informacje.



### Rozszerzenia informacji

Zmiany w Centrum informacyjnym dotyczącym sieci VPN w systemie V5R3 obejmują prezentację wizualną objaśniającą pojęcie dobrowolnego tunelu protokołu L2TP (Layer 2 Tunnel Protocol). Użyj następującego odsyłacza, aby zapoznać się z prezentacją wizualną dotyczącą Dobrowolnych tuneli L2TP zabezpieczanych protokołem IPSec.

Wymaga ona modułu dodatkowego Flash . Dostępna jest również wersja HTML tej prezentacji.

### Jak odróżnić nowości i zmiany

Aby pomóc w rozróżnieniu dokonanych zmian technicznych wykorzystano:

- Symbol  oznaczający początek informacji nowych lub zmienionych.
- Symbol  oznaczający koniec informacji nowych lub zmienionych.

Więcej informacji na temat nowości i zmian w tej wersji zawiera dokument Informacje dla użytkowników.



---

## Drukowanie tego dokumentu

Aby wyświetlić lub pobrać ten dokument w formacie PDF, wybierz Wirtualne sieci prywatne (VPN) (około 509 kB).

### Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Prawym przyciskiem myszy kliknij plik PDF w oknie przeglądarki (kliknij prawym przyciskiem myszy powyższy odsyłacz).
2. Jeśli używasz przeglądarki Internet Explorer, kliknij **Zapisz jako...**. Jeśli używasz przeglądarki Netscape Communicator, kliknij **Zapisz odsyłacz jako...**
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij przycisk **Zapisz**.

### Pobieranie programu Adobe Acrobat Reader

Do przeglądania lub drukowania tych plików PDF niezbędny jest program Adobe Acrobat Reader. Kopię tego programu można pobrać z serwisu internetowego firmy Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))



---

## Scenariusze dla sieci VPN

Aby poznać szczegóły techniczne i konfiguracyjne dotyczące każdego z podstawowych typów połączeń, należy przejrzeć następujące scenariusze:

- **“Scenariusz VPN: Podstawowe połączenie z biurem oddziału” na stronie 4**  
W scenariuszu tym opisano sytuację, w której przedsiębiorstwo zamierza nawiązać połączenie VPN pomiędzy podsieciami w dwóch odległych działach poprzez dwa komputery iSeries<sup>(TM)</sup> działające jako bramy VPN.
- **“Scenariusz VPN: Podstawowe połączenie pomiędzy firmami” na stronie 8**  
W tym scenariuszu przedsiębiorstwo chce nawiązać połączenie VPN pomiędzy kliencką stacją roboczą w swoim dziale produkcyjnym i kliencką stacją roboczą w dziale dostaw swojego kontrahenta.
- **“Scenariusz VPN: Ochrona dobrowolnego tunelu L2TP za pomocą protokołu IPSec” na stronie 13**  
Ten scenariusz przedstawia połączenie pomiędzy hostem w biurze oddziału a biurem centrali, wykorzystujące protokół L2TP zabezpieczony protokołem IPSec. Adres IP biura oddziału jest przypisywany dynamicznie, natomiast biuro główne ma statyczny, globalny adres IP.
- **“Scenariusz VPN: Wykorzystanie translacji adresów sieciowych na potrzeby sieci VPN” na stronie 19**  
W tym scenariuszu przedsiębiorstwo zamierza używać modułu OS/400<sup>(R)</sup> VPN do wymiany poufnych danych z jednym ze swoich partnerów handlowych. W celu dodatkowego zabezpieczenia swoich zasobów, przedsiębiorstwo chce także wykorzystać translację NAT w sieci VPN, aby ukryć przed aplikacjami, do których mają dostęp partnerzy, prywatny adres IP serwera używanego w roli hosta tych aplikacji.

### Dodatkowe scenariusze dla sieci VPN

Więcej scenariuszy konfiguracji sieci VPN można znaleźć w innych źródłach informacji poświęconych sieciom VPN:

- **Scenariusz: Bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usługi)**  
W sieciach VPN można tworzyć strategie dla mechanizmów usług QoS. W tym przykładzie przedstawiono wykorzystanie obydwu technologii.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM<sup>(R)</sup> e(logo)server iSeries Server with Windows<sup>(R)</sup> 2000 VPN Clients, REDP0153**



W tej dokumentacji technicznej firmy IBM przedstawiono, krok po kroku, proces konfigurowania tunelu komunikacyjnego VPN za pomocą modułu V5R1 VPN oraz zintegrowanej z systemem Windows 2000 obsługi protokołów L2TP i IPSec.

- **AS/400<sup>(R)</sup> Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**



W tej dokumentacji technicznej przedstawiono koncepcje dotyczące sieci VPN oraz opisano ich implementację za pomocą protokołów IPsec i L2TP (Layer 2 Tunneling Protocol) w systemie OS/400.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**



W dokumencie tym opisano wszystkie zintegrowane sieciowe opcje zabezpieczające dostępne w systemie OS/400, takie jak filtry IP, translację NAT, sieci VPN, serwer proxy HTTP, protokół SSL, usługi DNS, przekazywanie poczty, kontrolę i protokołowanie. Praktyczne wykorzystanie tych opcji przedstawiono w nim w formie przystępnych przykładów.

## Scenariusz VPN: Podstawowe połączenie z biurem oddziału

Przypuśćmy, że przedsiębiorstwo chce zminimalizować koszty komunikacji ze swoimi oddziałami oraz komunikacji pomiędzy tymi oddziałami. Obecnie w przedsiębiorstwie tym są używane łącza frame relay oraz linie dzierżawione, jednak zamierza ono zbadać inne opcje transmisji wewnętrznych, poufnych informacji - tańsze, bezpieczniejsze i zapewniające globalny dostęp. Wykorzystując Internet można w prosty sposób stworzyć wirtualną sieć prywatną (VPN), która zaspokoi potrzeby przedsiębiorstwa.

Zarówno firma, jak i jej oddziały wymagają ochrony łączy sieci VPN w Internecie, nie zaś w swoich wewnętrznych sieciach intranetowych. Jeśli przyjąć, że sieci intranetowe są sieciami zaufanymi, najlepszym rozwiązaniem będzie utworzenie sieci VPN od bramy do bramy. W takim wypadku obie bramy są podłączone bezpośrednio do sieci pośredniczącej. Innymi słowy są one systemami *granicznymi* lub *brzegowymi*, niezabezpieczonymi przez firewalle. Poniższy przykład wprowadza w czynności związane z przygotowaniem podstawowej konfiguracji sieci VPN. W scenariuszu tym, każde odwołanie do terminu *Internet* oznacza odwołanie do sieci pośredniczącej pomiędzy dwiema bramami VPN, którą może być zarówno własna sieć prywatna przedsiębiorstwa, jak i sieć Internet.

### Ważna uwaga:

W omawianym scenariuszu przedstawiono bramy ochrony iSeries<sup>(TM)</sup> podłączone bezpośrednio do Internetu. Nieuwzględnienie firewalli ma na celu uproszczenie scenariusza. Nie oznacza to jednak, że firewalle nie są konieczne. W rzeczywistości należy liczyć się z zagrożeniami bezpieczeństwa systemu podczas każdego połączenia z Internetem. Szczegółowy opis różnych sposobów redukcji tych zagrożeń zawiera dokumentacja

techniczna AS/400<sup>(R)</sup> Internet Security Scenarios: A Practical Approach, SG24-5954-00 

### Zalety

Poniższy scenariusz ma następujące zalety:

- Wykorzystanie Internetu lub istniejących sieci intranetowych obniża koszty prywatnych łączy pomiędzy odległymi podsieciami.
- Wykorzystanie Internetu lub istniejących sieci intranetowych zmniejsza poziom komplikacji wynikający z konieczności instalowania i utrzymania łączy prywatnych oraz związanego z nimi sprzętu.
- Wykorzystanie Internetu umożliwia łączenie się z odległymi sieciami z niemal dowolnego miejsca na świecie.
- Wykorzystanie sieci VPN zapewnia użytkownikom dostęp do wszystkich serwerów i zasobów z każdej strony połączenia w taki sam sposób, jak poprzez linie dzierżawione lub sieci rozległe (WAN).
- Wykorzystanie standardowych metod szyfrowania i uwierzytelniania zapewnia ochronę poufnych informacji przesyłanych z jednego miejsca w inne.
- Dynamiczna i regularna wymiana kluczy szyfrowania upraszcza konfigurację i minimalizuje ryzyko zdekodowania kluczy i naruszenia systemu ochrony.
- Wykorzystanie prywatnych adresów IP w każdej zdalnej podsieci eliminuje konieczność przydzielania każdemu klientowi cennych publicznych adresów IP.

## Cele

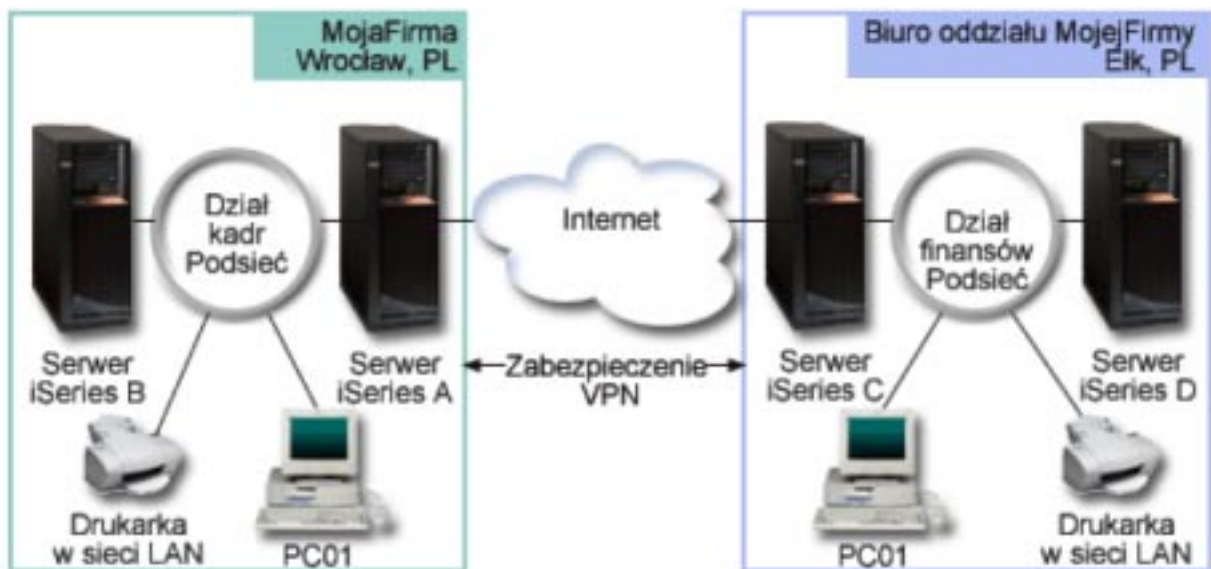
W tym scenariuszu firma MojaFirma zamierza stworzyć sieć VPN pomiędzy podsieciami swojego działu kadr i działu finansów poprzez parę serwerów iSeries. Obydwa serwery będą działały jako bramy sieci VPN. W konfiguracji VPN bramy zarządzają kluczami i stosują protokół IPSec do danych przesyłanych tunelem. Bramy nie są punktami końcowymi danych przesyłanych w tym połączeniu.

Cele tego scenariusza są następujące:

- Sieć VPN musi zabezpieczać cały ruch danych pomiędzy podsiecią działu kadr a podsiecią działu finansów.
- Przesyłane dane nie wymagają zabezpieczenia VPN po dotarciu do podsieci dowolnego działu.
- Wszystkie hosty i wszyscy klienci w jednej sieci mają pełny dostęp do drugiej sieci, w tym również dostęp do wszystkich aplikacji.
- Serwery bram mogą komunikować się ze sobą i mają dostęp do swoich aplikacji.

## Szczegóły

Poniższy rysunek ilustruje właściwości sieci firmy MojaFirma.



### Dział kadr

- Serwer iSeries-A działa pod kontrolą systemu operacyjnego OS/400<sup>(R)</sup> wersja 5 wydanie 2 (V5R2) i pełni rolę bramy sieci VPN działu personalnego.
- Adres IP podsieci to 10.6.0.0 z maską 255.255.0.0. Podsieć ta stanowi punkt końcowy danych przesyłanych tunelem VPN do oddziału firmy MojaFirma we Wrocławiu.
- Serwer iSeries-A łączy się z Internetem i ma adres IP 204.146.18.227. Stanowi on punkt końcowy połączenia. Oznacza to, że serwer iSeries-A zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP.
- Od strony podsieci adres IP serwera iSeries-A to 10.6.11.1.
- Serwer iSeries-B to serwer produkcyjny w podsieci działu kadr, na którym działają standardowe aplikacje TCP/IP.

### Dział finansów

- Serwer iSeries-C działa pod kontrolą systemu operacyjnego OS/400 wersja 5 wydanie 2 (V5R2) i pełni rolę bramy sieci VPN działu finansów.

- Adres IP podsieci to 10.196.8.0 z maską 255.255.255.0. Podsieć ta stanowi punkt końcowy danych przesyłanych tunelem VPN do oddziału firmy MojaFirma w Krakowie.
- Serwer iSeries-C łączy się z Internetem i ma adres IP 208.222.150.250. Stanowi on punkt końcowy połączenia. Oznacza to, że serwer iSeries-C zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP.
- Serwer iSeries-C ma od strony podsieci adres IP 10.196.8.5.

### Krok 1: Zadania konfiguracyjne

Aby skonfigurować połączenie z biurem oddziału opisane w tym scenariuszu, należy wykonać każde z poniższych zadań konfiguracyjnych:

1. Sprawdź, czy routing TCP/IP umożliwi obydwu serwerom bram komunikowanie się ze sobą poprzez Internet. Dzięki temu hosty w każdej podsieci będą prawidłowo kierować do swojej bramy żądania dostępu do zdalnej podsieci.  
**Uwaga:** Zagadnienia związane z konfigurowaniem routingu wykraczają poza zakres tej sekcji. Jeśli masz jakiegokolwiek wątpliwości, zapoznaj się z sekcją Routing TCP/IP i równoważenie obciążeń w Centrum informacyjnym.
2. Wypełnij (Str. 6) arkusze planowania i listy kontrolne dla obydwu systemów.
3. Skonfiguruj (Str. 7) ustawienia sieci VPN na serwerze bramy VPN działu kadr (iSeries-A).
4. Skonfiguruj (Str. 8) ustawienia sieci VPN na serwerze bramy VPN działu finansów (iSeries-C).
5. Sprawdź, czy serwery VPN zostały uruchomione (Str. 8).
6. Przetestuj (Str. 8) komunikację pomiędzy dwiema odległymi podsieciami.

### Szczegóły konfigurowania

Po wykonaniu pierwszej czynności, czyli sprawdzeniu, czy routing TCP/IP działa prawidłowo i czy serwery bram mogą komunikować się ze sobą, można przystąpić do konfigurowania sieci VPN.

### Krok 2: Wypełnienie arkusza planowania

Przedstawione poniżej listy kontrolne związane z planowaniem wskazują rodzaje informacji, które należy zebrać przed rozpoczęciem konfigurowania sieci VPN. Rozpoczęcie czynności konfiguracyjnych jest możliwe tylko wtedy, gdy wszystkie odpowiedzi na pytania zawarte na liście kontrolnej wymagań wstępnych brzmią TAK.

**Uwaga:** Poniższe arkusze dotyczą serwera iSeries-A; procedurę należy powtórzyć dla serwera iSeries-C, odpowiednio zmieniając adresy IP.

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy system operacyjny to OS/400 <sup>(R)</sup> wersja V5R2 (5722-SS1) lub nowsza?	Tak
Czy zainstalowano opcję Digital Certificate Manager (5722-SS1 opcja 34)?	Tak
Czy zainstalowano produkt Cryptographic Access Provider (5722-AC2 lub AC3)?	Tak
Czy zainstalowano produkt iSeries <sup>(TM)</sup> Access for Windows <sup>(R)</sup> (5722-XE1)?	Tak
Czy zainstalowano program iSeries Navigator?	Tak
Czy zainstalowano komponent Sieć programu iSeries Navigator?	Tak
Czy zainstalowano produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy na serwerze iSeries skonfigurowano protokół TCP/IP (w tym interfejsy IP, trasy, nazwę lokalnego hosta i nazwę lokalnej domeny)?	Tak
Czy pomiędzy obydwoma punktami końcowymi nawiązano normalne połączenie TCP/IP?	Tak
Czy zastosowano najnowsze poprawki PTF?	Tak
Czy w wypadku, kiedy tunel VPN przechodzi przez firewalle lub routery korzystające z filtracji pakietów IP, reguły filtrowania firewalla lub routera obsługują protokoły AH i ESP?	Tak

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy konfiguracja firewalli lub routerów umożliwia stosowanie protokołów IKE (port UDP 500), AH i ESP?	Tak
Czy konfiguracja firewalli umożliwia przekazywanie IP?	Tak

Informacje potrzebne do skonfigurowania połączenia VPN	Odpowiedzi
Jakiego typu połączenie jest tworzone?	Między bramami
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	HRgw2FINgw
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony kluczy?	Zrównoważonego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Nie scisletajne
Jaki jest identyfikator lokalnego serwera kluczy?	Adres IP: 204.146.18.227
Jaki jest identyfikator lokalnego punktu końcowego danych?	Podsieć: 10.6.0.0 Maska: 255.255.0.0
Jaki jest identyfikator zdalnego serwera kluczy?	Adres IP: 208.222.150.250
Jaki jest identyfikator zdalnego punktu końcowego danych?	Podsieć: 10.196.8.0 Maska: 255.255.255.0
Jakie protokoły i jakie porty mają być dostępne dla połączenia?	Dowolne
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony danych?	Zrównoważonego
Jakiego interfejsu dotyczy połączenie?	TRLINE

### Krok 3: Konfigurowanie sieci VPN na serwerze iSeries-A

Za pomocą informacji zawartych w arkuszach należy w następujący sposób skonfigurować ustawienia sieci VPN na serwerze iSeries-A:

1. W programie iSeries Navigator rozwiń pozycję iSeries-A →**Sieć** →**Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator nowych połączeń.
3. Na stronie **Powitanie** przeczytaj informacje o obiektach tworzonych przez kreator.
4. Kliknij przycisk **Dalej**, aby przejść do strony **Nazwa połączenia**.
5. W polu **Nazwa** wpisz HRgw2FINgw.
6. (opcjonalnie) Wprowadź opis tej grupy połączeń.
7. Kliknij przycisk **Dalej**, aby przejść do strony **Scenariusz połączenia**.
8. Wybierz pozycję **Połączenie bramy użytkownika z inną bramą**.
9. Kliknij przycisk **Dalej**, aby przejść do strony **Strategia protokołu IKE**.
10. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz **Równoważ ochronę i wydajność**.
11. Kliknij przycisk **Dalej**, aby przejść do strony **Certyfikat dla lokalnego punktu końcowego połączenia**.
12. Wybierz **Nie**, aby wskazać, że do uwierzytelniania tego połączenia nie będzie używany certyfikat.
13. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny serwer kluczy**.
14. W polu **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
15. W polu **Adres IP** wpisz 204.146.18.227.
16. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny serwer kluczy**.
17. W polu **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
18. W polu **Adres IP** wpisz 208.222.150.250.
19. W polu **Wstępny klucz wspólny** wpisz topsecretstuff.
20. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny punkt końcowy danych**.



21. W polu **Typ identyfikatora** wybierz pozycję **Podsieć IP wersja 4**.
22. W polu **Identyfikator** wpisz 10.6.0.0.
23. W polu **Maska podsieci** wpisz 255.255.0.0.
24. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny punkt końcowy danych**.
25. W polu **Typ identyfikatora** wybierz pozycję **Podsieć IP wersja 4**.
26. W polu **Identyfikator** wpisz 10.196.8.0.
27. W polu **Maska podsieci** wpisz 255.255.255.0.
28. Kliknij przycisk **Dalej**, aby przejść do strony **Usługi danych**.
29. Zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**, aby przejść do strony **Strategia danych**.
30. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz **Równoważ ochronę i wydajność**. Wybierz opcję **Użyj algorytmu szyfrowania RC4**.
31. Kliknij przycisk **Dalej**, aby przejść do strony **Dostępne interfejsy**.
32. Z tabeli **Wiersz** wybierz pozycję **TRLINE**.
33. Kliknij przycisk **Dalej**, aby przejść do strony **Podsumowanie**. Sprawdź, czy utworzone przez kreator obiekty są poprawne.
34. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie.
35. Po wyświetleniu okna dialogowego **Aktywacja filtrów strategii** wybierz odpowiedź **Tak, uaktywnij wygenerowane filtry strategii**, a następnie wybierz opcję **Przepuszczaj pozostały ruch**. Kliknij przycisk **OK**, aby zakończyć konfigurowanie. W wyświetlonym oknie dialogowym zaznacz, że reguły mają być uaktywnione dla wszystkich interfejsów.

Konfigurowanie sieci VPN dla serwera iSeries-A zostało zakończone. Kolejnym krokiem jest skonfigurowanie ustawień sieci VPN dla bramy VPN działu finansów (iSeries-C).

#### **Krok 4: Konfigurowanie ustawień sieci VPN dla serwera iSeries-C**

Należy powtórzyć te same czynności, które wykonano podczas konfigurowania serwera iSeries-A, zmieniając odpowiednio adresy IP. Odpowiednią pomoc zapewnią arkusze planowania. Po zakończeniu konfigurowania bramy VPN działu finansów połączenia będą w stanie *na żądanie*, co znaczy, że połączenie zostanie nawiązane po wysłaniu datagramów IP, które połączenie VPN musi chronić. Kolejnym krokiem jest uruchomienie serwerów VPN, o ile jeszcze nie zostały uruchomione.

#### **Krok 5: Uruchomienie serwerów VPN**

Aby uruchomić serwery VPN, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **serwer** → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Uruchom**.

#### **Krok 7: Testowanie połączenia**

Po skonfigurowaniu obydwu serwerów VPN i pomyślnym ich uruchomieniu przetestuj łączność, aby sprawdzić, czy odległe podsieci mogą się ze sobą komunikować. W tym celu wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** → **Sieć**.
2. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Narzędzia**, a następnie wybierz opcję **Ping**.
3. W polu **Ping** okna dialogowego **Ping z** wpisz iSeries-C.
4. Kliknij przycisk **Uruchom komendę Ping**, aby sprawdzić łączność pomiędzy serwerami iSeries-A i iSeries-C.
5. Po zakończeniu testu kliknij przycisk **OK**.

## **Scenariusz VPN: Podstawowe połączenie pomiędzy firmami**

Wiele przedsiębiorstw wykorzystuje łącza frame relay lub linie dzierżawione na potrzeby bezpiecznej komunikacji ze swoimi partnerami gospodarczymi, podmiotami podporządkowanymi i dostawcami. Niestety, tego rodzaju rozwiązania

są często kosztowne i mają ograniczony zasięg terytorialny. Sieci VPN oferują alternatywne rozwiązanie dla przedsiębiorstw potrzebujących prywatnych, ekonomicznych środków łączności.

Założmy, że dane przedsiębiorstwo jest głównym dostawcą części dla producenta. Ponieważ w takiej sytuacji ogromne znaczenie ma posiadanie określonych części w ilościach wymaganych przez producenta i dysponowanie nimi w odpowiednim czasie, dostawca musi na bieżąco znać stan zapasów producenta i jego harmonogramy produkcji. Nawet obecnie może się zdarzać, że informacje takie przekazuje się w sposób tradycyjny (telefonicznie, faksem), co jednak jest czasochłonne, kosztowne, a niekiedy może prowadzić do błędów. Dlatego firma dostawcza szuka prostszej, szybszej i efektywniejszej metody komunikacji ze swoim partnerem-producentem. Jednak ze względu na poufność i zmienność wymienianych informacji, producent nie chce publikować ich na swoim korporacyjnym serwerze internetowym, ani rozprowadzać w formie comiesięcznych raportów dla kontrahentów zewnętrznych. Wykorzystując Internet, można w prosty sposób utworzyć wirtualną sieć prywatną (VPN), która spełni wymagania obydwu przedsiębiorstw.

### Cele

W tym scenariuszu firma MojaFirma chce nawiązać połączenie VPN pomiędzy hostem w swoim dziale podzespołów a hostem w dziale produkcji jednego ze swoich kontrahentów, firmy InnaFirma.

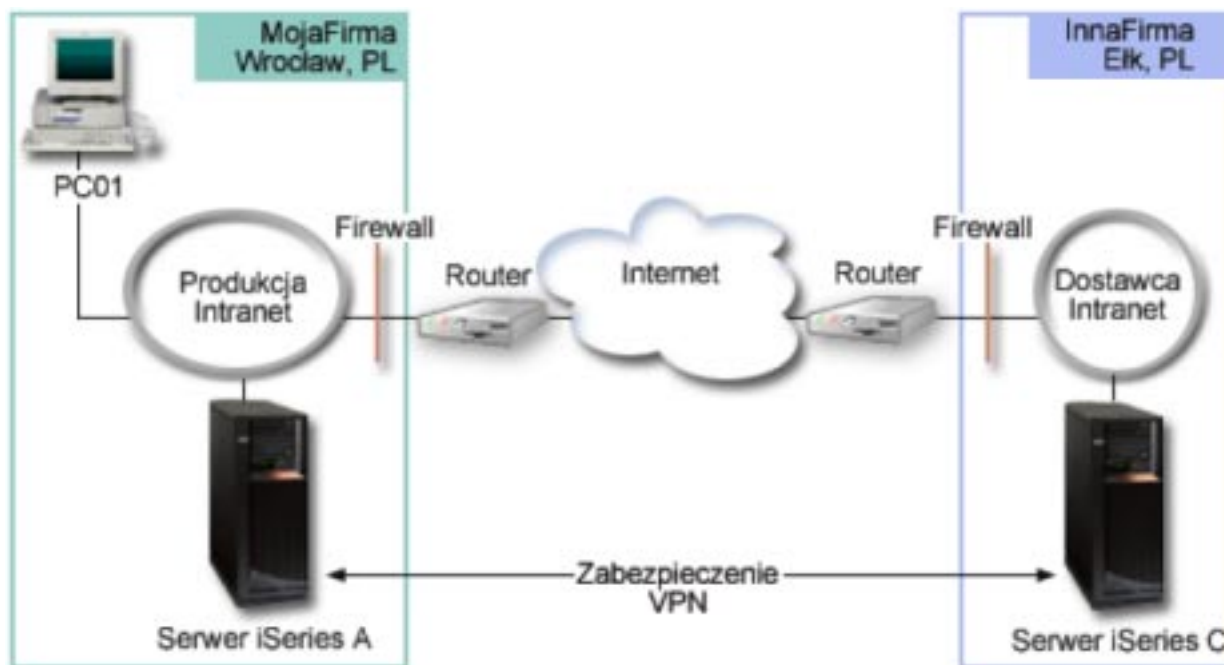
Ponieważ współużytkowane przez obydwie firmy informacje mają charakter ściśle poufny, konieczne jest ich zabezpieczenie w czasie przesyłania przez Internet. Także w sieciach obydwu firm dane nie mogą być przesyłane w postaci jawnej, ponieważ żadna z tych sieci nie uważa drugiej sieci za zaufaną. Innymi słowy, obie firmy wymagają uwierzytelniania, integralności i szyfrowania danych na całej trasie połączenia.

### Ważna uwaga:

Celem tego scenariusza jest zaprezentowanie w formie przykładu prostej konfiguracji sieci VPN między hostami. W typowym środowisku sieciowym trzeba także rozważyć między innymi skonfigurowanie firewalla oraz wymagania w zakresie adresów IP i routingu.

### Szczegóły

Poniższy rysunek ilustruje schemat sieci firm MojaFirma i InnaFirma.



### Sieć działu podzespołów firmy MojaFirma

- Serwer iSeries-A działa pod kontrolą systemu operacyjnego OS/400<sup>(R)</sup> wersja 5 wydanie 2 (V5R2).
- Serwer iSeries-A ma adres IP 10.6.1.1. Jest to punkt końcowy zarówno połączenia, jak i danych. Oznacza to, że serwer iSeries-A negocjuje parametry protokołu IKE oraz stosuje protokół IPSec do przychodzących i wychodzących datagramów IP, a także jest źródłem i miejscem docelowym danych przesyłanych poprzez sieć VPN.
- Serwer iSeries-A znajduje się w podsieci 10.6.0.0 z maską 255.255.0.0
- Tylko serwer iSeries-A może inicjować połączenia z serwerem iSeries-C.

### Sieć działu produkcji firmy InnaFirma

- Serwer iSeries-C działa pod kontrolą systemu operacyjnego OS/400 wersja 5 wydanie 2 (V5R2).
- Serwer iSeries-C ma adres IP 10.196.8.6. Jest to punkt końcowy zarówno połączenia, jak i danych. Oznacza to, że serwer iSeries-A negocjuje parametry protokołu IKE oraz stosuje protokół IPSec do przychodzących i wychodzących datagramów IP, a także jest źródłem i miejscem docelowym danych przesyłanych poprzez sieć VPN.
- Serwer iSeries-C znajduje się w podsieci 10.196.8.0 z maską 255.255.255.0

### Krok 1: Zadania konfiguracyjne

Aby skonfigurować opisane w tym scenariuszu połączenie między firmami, wykonaj wszystkie poniższe zadania konfiguracyjne:

1. Sprawdź, czy routing TCP/IP umożliwia serwerom iSeries-A i iSeries-C komunikowanie się ze sobą poprzez Internet. Dzięki temu hosty w każdej podsieci będą prawidłowo kierować do swojej bramy żądania dostępu do zdalnej podsieci. Weź pod uwagę fakt, że w tym scenariuszu konieczny będzie routing adresów prywatnych, który wcześniej nie był potrzebny.

**Uwaga:** Zagadnienia konfigurowania routingu wykraczają poza zakres tej sekcji. Jeśli masz jakiegokolwiek wątpliwości, zapoznaj się z sekcją Routing TCP/IP i równoważenie obciążeń w Centrum informacyjnym.

2. Wypełnij (Str. 10) arkusze planowania i listy kontrolne dla obydwu systemów.
3. Skonfiguruj (Str. 11) ustawienia sieci VPN na serwerze iSeries-A w sieci działu podzespołów firmy MojaFirma.
4. Skonfiguruj (Str. 12) ustawienia sieci VPN na serwerze iSeries-C w sieci działu produkcji firmy InnaFirma.
5. Uaktywnij (Str. 12) reguły filtrowania na obydwu serwerach.
6. Uruchom (Str. 13) połączenie z serwera iSeries-A.
7. Przetestuj (Str. 13) komunikację pomiędzy dwiema odległymi podsieciami.

### Szczegóły konfigurowania

Po wykonaniu pierwszej czynności, to jest sprawdzeniu, czy routing TCP/IP działa prawidłowo i czy serwery mogą komunikować się ze sobą, można przystąpić do konfigurowania sieci VPN.

### Krok 2: Wypełnienie arkusza planowania

Przedstawione poniżej listy kontrolne związane z planowaniem wskazują rodzaje informacji, które należy zebrać przed rozpoczęciem konfigurowania sieci VPN. Rozpoczęcie czynności konfiguracyjnych jest możliwe tylko wtedy, gdy wszystkie odpowiedzi na pytania zawarte na liście kontrolnej wymagań wstępnych brzmią TAK.

**Uwaga:** Poniższe arkusze dotyczą serwera iSeries-A; procedurę należy powtórzyć dla serwera iSeries-C, odpowiednio zmieniając adresy IP.

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy system operacyjny to OS/400 <sup>(R)</sup> wersja V5R2 (5722-SS1) lub nowsza?	Tak
Czy zainstalowano opcję Digital Certificate Manager (5722-SS1 opcja 34)?	Tak
Czy zainstalowano produkt Cryptographic Access Provider (5722-AC2 lub AC3)?	Tak
Czy zainstalowano produkt iSeries <sup>(TM)</sup> Access for Windows <sup>(R)</sup> (5722-XE1)?	Tak
Czy zainstalowano program iSeries Navigator?	Tak
Czy zainstalowano komponent Sieć programu iSeries Navigator?	Tak



Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy zainstalowano produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy na serwerze iSeries skonfigurowano protokół TCP/IP (w tym interfejsy IP, trasy, nazwę lokalnego hosta i nazwę lokalnej domeny)?	Tak
Czy pomiędzy obydwojoma punktami końcowymi nawiązano normalne połączenie TCP/IP?	Tak
Czy zastosowano najnowsze poprawki PTF?	Tak
Czy w wypadku, kiedy tunel VPN przechodzi przez firewalle lub routery korzystające z filtracji pakietów IP, reguły filtrowania firewalla lub routera obsługują protokoły AH i ESP?	Tak
Czy konfiguracja firewalle lub routerów umożliwia stosowanie protokołów IKE (port UDP 500), AH i ESP?	Tak
Czy konfiguracja firewalle umożliwia przekazywanie IP?	Tak

Informacje potrzebne do skonfigurowania połączenia VPN	Odpowiedzi
Jakiego typu połączenie jest tworzone?	Między hostami
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	MojaFirmaDoInnaFirma
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony kluczy?	Najwyższego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Tak
Jaki jest identyfikator lokalnego serwera kluczy?	Adres IP: 10.6.1.1
Jaki jest identyfikator lokalnego punktu końcowego danych?	Adres IP: 10.6.1.1
Jaki jest identyfikator zdalnego serwera kluczy?	Adres IP: 10.196.8.6
Jaki jest identyfikator zdalnego punktu końcowego danych?	Adres IP: 10.196.8.6
Jakie protokoły i jakie porty mają być dostępne dla połączenia?	Dowolne
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony danych?	Najwyższego
Jakiego interfejsu dotyczy połączenie?	TRLINE

### Krok 3: Konfigurowanie sieci VPN na serwerze iSeries-A

Za pomocą informacji zawartych w arkuszach należy w następujący sposób skonfigurować ustawienia sieci VPN na serwerze iSeries-A:

1. W programie iSeries Navigator rozwin pozycję serwer —>**Sieć** —>**Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator połączeń.
3. Na stronie **Powitanie** przeczytaj informacje o obiektach tworzonych przez kreator.
4. Kliknij przycisk **Dalej**, aby przejść do strony **Nazwa połączenia**.
5. W polu **Nazwa** wpisz **MojaFirmaDoInnaFirma**.
6. (opcjonalnie) Wprowadź opis tej grupy połączeń.
7. Kliknij przycisk **Dalej**, aby przejść do strony **Scenariusz połączenia**.
8. Wybierz pozycję **Połącz lokalny host z innym hostem**.
9. Kliknij przycisk **Dalej**, aby przejść do strony **Strategia protokołu IKE**.
10. Wybierz **Utwórz nową strategię**, a następnie wybierz **Najwyższa ochrona, najniższa wydajność**.
11. Kliknij przycisk **Dalej**, aby przejść do strony **Certyfikat dla lokalnego punktu końcowego połączenia**.
12. Wybierz **Tak**, aby wskazać, że do uwierzytelniania tego połączenia będą używane certyfikaty. Następnie wybierz certyfikat, który będzie odpowiadał serwerowi iSeries-A.

**Uwaga:** Aby używać certyfikatu do uwierzytelniania lokalnego punktu końcowego połączenia, należy najpierw utworzyć ten certyfikat w Menedżerze certyfikatów cyfrowych (DCM).

13. Kliknij przycisk **Dalej**, aby przejść do strony **Identyfikator lokalnego punktu końcowego połączenia**.
14. Jako typ identyfikatora wybierz **Adres IP wersja 4**. Przypisanym adresem IP musi być adres 10.6.1.1. Informacje te zostały również zdefiniowane w certyfikacie utworzonym w programie DCM.
15. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny serwer kluczowy**.
16. W polu **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
17. W polu **Identyfikator** wpisz 10.196.8.6.
18. Kliknij przycisk **Dalej**, aby przejść do strony **Usługi danych**.
19. Zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**, aby przejść do strony **Strategia danych**.
20. Wybierz **Utwórz nową strategię**, a następnie wybierz **Najwyższa ochrona, najniższa wydajność**. Wybierz opcję **Użyj algorytmu szyfrowania RC4**.
21. Kliknij przycisk **Dalej**, aby przejść do strony **Dostępne interfejsy**.
22. Wybierz pozycję **TRLINE**.
23. Kliknij przycisk **Dalej**, aby przejść do strony **Podsumowanie**. Sprawdź, czy utworzone przez kreator obiekty są poprawne.
24. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie.
25. Po wyświetleniu okna dialogowego **Uaktywnienie filtrów strategii** wybierz odpowiedź **Nie, reguły pakietów zostaną uaktywnione później**, a następnie kliknij przycisk **OK**.

W kolejnym kroku należy zaznaczyć, że tylko serwer iSeries-A może zainicjować to połączenie. W tym celu należy dostosować właściwości grupy z kluczem dynamicznym MojaFirmaDoInnaFirma utworzonej przez kreator:

1. Kliknij pozycję **Według grupy** po lewej stronie interfejsu VPN. Po prawej stronie zostanie wyświetlona grupa z kluczem dynamicznym MojaFirmaDoInnaFirma. Kliknij ją prawym przyciskiem myszy i wybierz opcję **Właściwości**.
2. Przejdź do strony **Strategia** i wybierz opcję **Połączenie inicjuje system lokalny**.
3. Kliknij **OK**, aby zapisać wprowadzone zmiany.

Konfigurowanie sieci VPN dla serwera iSeries-A zostało zakończone. Kolejnym krokiem jest skonfigurowanie sieci VPN dla serwera iSeries-C w sieci działu produkcji firmy InnaFirma.

#### **Krok 4: Konfigurowanie ustawień sieci VPN dla serwera iSeries-C**

Należy powtórzyć te same czynności, które wykonano podczas konfigurowania serwera iSeries-A, zmieniając odpowiednio adresy IP. Odpowiednią pomoc zapewnią arkusze planowania. Po skonfigurowaniu serwera iSeries-C należy uaktywnić reguły filtrowania utworzone przez Kreator połączeń dla każdego serwera.

#### **Krok 5: Uaktywnienie reguł pakietów**

Kreator automatycznie tworzy reguły pakietów wymagane do poprawnego działania tego połączenia. Zanim jednak będzie można uruchomić połączenie VPN, należy je uaktywnić na obydwu serwerach. W tym celu wykonaj następujące czynności na serwerze iSeries-A:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** —>**Sieć** —>**Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Uaktywnij**. Spowoduje to utworzenie okna dialogowego **Uaktywnij reguły pakietów**.
3. Wybierz uaktywnienie wyłącznie wygenerowanych reguł VPN, wyłącznie wybranego pliku lub zarówno wygenerowanych reguł VPN, jak i wybranego pliku. Można wybrać ostatnią opcję, aby na przykład wymusić na interfejsie różne reguły typu PERMIT i DENY, oprócz wygenerowanych reguł VPN.
4. Wybierz interfejs, dla którego chcesz uaktywnić reguły. W tym wypadku wybierz opcję **Wszystkie interfejsy**.
5. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić zamiar weryfikacji i uaktywnienia reguł dla określonych interfejsów. Po kliknięciu przycisku OK system sprawdzi składniową i semantyczną poprawność reguł

oraz wyświetli wyniki w oknie komunikatu u dołu edytora. W wypadku komunikatów o błędach dotyczących określonego pliku i numeru wiersza można kliknąć dany komunikat prawym przyciskiem myszy i wybrać opcję **Przejdź do wiersza**, aby wyróżnić błąd w pliku.

6. Powtórz powyższe czynności, aby uaktywnić reguły pakietów na serwerze iSeries-C.

#### Krok 6: Uruchomienie połączenia

Aby uruchomić połączenie MojaFirmaDoInnaFirma z serwera iSeries-A, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** → **Sieć** → **Strategie IP**.
2. Jeśli serwer VPN nie jest uruchomiony, kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Uruchom**. Spowoduje to uruchomienie serwera sieci VPN.
3. Rozwiń pozycję **Sieć VPN** → **Połączenia chronione**.
4. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
5. Kliknij prawym przyciskiem myszy pozycję **MojaFirmaDoInnaFirma** i wybierz opcję **Uruchom**.
6. Z menu **Widok** wybierz opcję **Odśwież**. Jeśli połączenie zostało uruchomione pomyślnie, jego status zmieni się z wartości *Bezczynne* na *Włączone*. Uruchomienie połączenia może trwać kilka minut, więc należy okresowo odświeżać status, dopóki nie przyjmie on wartości *Włączone*.

#### Krok 7: Testowanie połączenia

Po skonfigurowaniu obydwu serwerów i pomyślnym uruchomieniu połączenia przetestuj łączność, aby sprawdzić, czy odległe hosty mogą się ze sobą komunikować. W tym celu wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** → **Sieć**.
2. Prawym przyciskiem myszy kliknij pozycję **Konfiguracja TCP/IP** i wybierz opcję **Narzędzia**, a następnie wybierz opcję **Ping**.
3. W polu **Ping** okna dialogowego **Ping z** wpisz iSeries-C.
4. Kliknij przycisk **Uruchom komendę Ping**, aby sprawdzić łączność pomiędzy serwerami iSeries-A i iSeries-C.
5. Po zakończeniu testu kliknij przycisk **OK**.

## Scenariusz VPN: Ochrona dobrowolnego tunelu L2TP za pomocą protokołu IPsec

Załóżmy, że przedsiębiorstwo ma niewielki oddział w innym regionie. W czasie każdego dnia pracy pracownicy oddziału potrzebują dostępu do poufnych informacji przechowywanych na serwerze iSeries<sup>(TM)</sup> działającym w sieci intranetowej przedsiębiorstwa. Obecnie przedsiębiorstwo wykorzystuje do tego celu drogie linie dzierżawione. Mimo że firma chce w dalszym ciągu oferować bezpieczny dostęp do swojego intranetu, przede wszystkim pragnie obniżyć koszty związane z linią dzierżawioną. Aby to zrobić, może utworzyć dobrowolny (voluntary) tunel L2TP (Layer 2 Tunnel Protocol), który rozszerzy sieć korporacyjną w taki sposób, że biuro oddziału będzie wyglądało jak część korporacyjnej podsieci. Ruch danych przez tunel L2TP będzie zabezpieczony przez sieć VPN.

W ramach dobrowolnego tunelu L2TP biuro odległego oddziału ustanowi tunel bezpośrednio do sieciowego serwera L2TP (LNS) w sieci korporacyjnej. Funkcje koncentratora dostępu L2TP (LAC) rezydują po stronie klienta. Tunel jest przezroczysty dla dostawców ISP zdalnych klientów, więc dostawcy ci nie muszą obsługiwać protokołu L2TP. Więcej informacji na temat protokołu L2TP zawiera sekcja “Protokół Layer 2 Tunnel Protocol (L2TP)” na stronie 26.

#### Ważna uwaga:

W omawianym scenariuszu przedstawiono bramy ochrony iSeries podłączone bezpośrednio do Internetu. Nieuwzględnienie firewalli ma na celu uproszczenie scenariusza. Nie oznacza to jednak, że firewallle nie są konieczne. Należy liczyć się z zagrożeniami bezpieczeństwa systemu podczas każdego połączenia z Internetem. Szczegółowy opis różnych sposobów redukcji tych zagrożeń zawiera dokumentacja techniczna AS/400<sup>(R)</sup>

Internet Security Scenarios: A Practical Approach, SG24-5954-00 

Cele

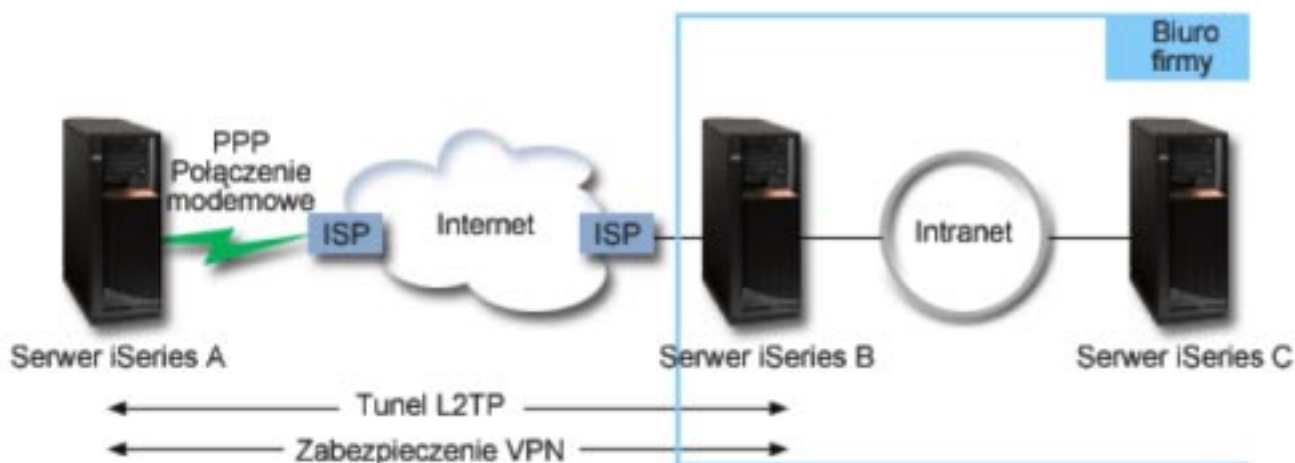
W tym scenariuszu serwer iSeries znajdujący się w oddziale firmy łączy się tunelem L2TP zabezpieczonym przez sieć VPN z siecią korporacyjną tej firmy przez bramę na serwerze iSeries.

Główne cele tego scenariusza to:

- System w biurze oddziału zawsze inicjuje połączenie z główną siedzibą firmy.
- System w biurze oddziału jest jedynym systemem w sieci oddziału, który potrzebuje dostępu do sieci korporacyjnej. Oznacza to, że działa on w sieci oddziału w roli hosta, a nie bramy.
- System korporacyjny jest hostem w sieci korporacyjnej.

**Szczegóły**

Poniższy rysunek ilustruje schemat sieci w tym scenariuszu:



#### Serwer iSeries-A

- Musi mieć dostęp do aplikacji TCP/IP we wszystkich systemach sieci korporacyjnej.
- Otrzymuje dynamicznie przypisywane adresy IP od dostawcy ISP.
- Musi być skonfigurowany do obsługi L2TP.

#### Serwer iSeries-B

- Musi mieć dostęp do aplikacji TCP/IP na serwerze iSeries-A.
- Adres IP podsieci to 10.6.0.0 z maską 255.255.0.0. Ta podsieć reprezentuje punkt końcowy danych tunelu VPN w siedzibie głównej.
- Od strony Internetu ma adres IP 205.13.237.6. Stanowi on punkt końcowy połączenia. Oznacza to, że serwer iSeries-B zarządza kluczami i stosuje protokół IPsec do przychodzących i wychodzących datagramów IP. Od strony podsieci adres IP serwera iSeries-B to 10.6.11.1.

Zgodnie z terminologią właściwą dla protokołu L2TP serwer *iSeries-A* działa jako inicjator L2TP, podczas gdy serwer *iSeries-B* działa jako terminator L2TP.

#### Krok 1: Zadania konfiguracyjne

Zakładając, że protokół TCP/IP jest już skonfigurowany i działa, wykonaj następujące zadania:

1. Skonfiguruj ustawienia sieci VPN (Str. 15) na serwerze iSeries-A.
2. Skonfiguruj profil połączenia PPP (Str. 17) i linię wirtualną dla serwera iSeries-A.
3. Wprowadź (Str. 18) grupę z kluczem dynamicznym do profilu PPP.
4. Skonfiguruj ustawienia sieci VPN (Str. 18) na serwerze iSeries-B.
5. Skonfiguruj profil połączenia PPP (Str. 18) i linię wirtualną dla serwera iSeries-B.

6. Uaktywnij (Str. 19) reguły pakietów na serwerach iSeries-A i iSeries-B.
7. Uruchom (Str. 19) połączenie z serwera iSeries-A.

## Szczegóły konfigurowania

Po sprawdzeniu, czy protokół TCP/IP działa prawidłowo i czy serwery iSeries<sup>(TM)</sup> mogą komunikować się ze sobą, można przystąpić do konfigurowania połączenia opisanego w niniejszym scenariuszu.

### Krok 1: Konfigurowanie sieci VPN na serwerze iSeries-A

Aby skonfigurować sieć VPN na serwerze iSeries-A, wykonaj następujące czynności:

#### 1. Konfigurowanie strategii protokołu Internet Key Exchange

- a. W programie iSeries Navigator rozwiń pozycję iSeries-A → **Sieć** → **Strategie IP** → **Sieć VPN** → **Strategia ochrony IP**.
- b. Prawym przyciskiem myszy kliknij pozycję **Strategia protokołu Internet Key Exchange** i wybierz opcję **Nowa strategia protokołu Internet Key Exchange**.
- c. Na stronie **Zdalny serwer** wybierz pozycję **Adres IP wersja 4** jako typ identyfikatora, a następnie wpisz 205.13.237.6 w polu **Adres IP**.
- d. Na stronie **Powiązania** wybierz **Wstępny klucz współużytkowany**, aby wskazać, że połączenie używa wstępnego klucza współużytkowanego do uwierzytelniania tej strategii.
- e. W polu **Klucz** wpisz nazwę wstępnego klucza współużytkowanego. Wstępny klucz współużytkowany należy traktować tak, jak hasło.
- f. Wybierz pozycję **Identyfikator klucza** jako typ identyfikatora lokalnego serwera kluczy, a następnie wpisz identyfikator klucza w polu **Identyfikator**. Na przykład ToJestIdKlucza. Należy pamiętać, że lokalny serwer kluczy ma dynamicznie przypisywany adres IP, którego nie można z góry przewidzieć. Serwer iSeries-B używa tego identyfikatora do identyfikacji serwera iSeries-A, gdy ten inicjuje połączenie.
- g. Na stronie **Transformacje** kliknij przycisk **Dodaj**, aby dodać transformacje proponowane serwerowi iSeries-B przez serwer iSeries-A w celu ochrony klucza i aby określić, czy strategia protokołu IKE wykorzystuje ochronę tożsamości podczas inicjowania fazy 1. negocjacji.
- h. Na stronie **Transformacja strategii IKE** wybierz opcję **Wstępny klucz współużytkowany** jako metodę uwierzytelniania, **SHA** jako algorytm mieszający i **3DES-CBC** jako algorytm szyfrowania. Zaakceptuj wartości domyślne dla grupy Diffie-Hellman oraz dla pozycji Unieważnij klucze IKE po upływie.
- i. Kliknij przycisk **OK**, aby powrócić do strony **Transformacje**.
- j. Wybierz opcję **Agresywny tryb negocjacji IKE (bez ochrony tożsamości)**.  
➤ **Uwaga:** Jeśli w konfiguracji jednocześnie używane są wstępne klucze współużytkowane i agresywny tryb negocjacji, należy wybrać trudne hasła, których nie można złamać podczas ataku ze słownikiem. Zaleca się również okresowe zmiany haseł. ⚡
- k. Kliknij przycisk **OK**, aby zapisać konfigurację.

#### 2. Konfigurowanie strategii danych

- a. W interfejsie VPN kliknij prawym przyciskiem myszy pozycję **Strategia danych** i wybierz opcję **Nowa strategia danych**.
- b. Na stronie **Ogólne** określ nazwę strategii danych. Na przykład ZdalnyUzytkownikL2TP.
- c. Przejdź do strony **Kolekcja propozycji**. Kolekcja propozycji to zbiór protokołów używanych przez inicjujący i odpowiadający serwer kluczy do nawiązania dynamicznego połączenia pomiędzy dwoma punktami końcowymi. Tę samą strategię danych można wykorzystać dla kilku obiektów połączeń. Jednak nie wszystkie zdalne serwery kluczy VPN muszą mieć takie same właściwości strategii danych. Dlatego można dodać kilka kolekcji propozycji do strategii danych. Podczas nawiązywania połączenia VPN ze zdalnym serwerem kluczy, w strategii danych inicjatora i respondenta musi być co najmniej jedna zgodna kolekcja propozycji.
- d. Kliknij przycisk **Dodaj**, aby dodać transformacje strategii danych.
- e. Wybierz pozycję **Transport** dla trybu hermetyzacji.
- f. Określ termin ważności klucza.
- g. Kliknij przycisk **OK**, aby powrócić do strony **Transformacje**.



h. Kliknij przycisk **OK**, aby zapisać nową strategię danych.

### 3. Konfigurowanie grupy z kluczem dynamicznym

4.

- a. W interfejsie VPN rozwiń pozycję **Bezpieczne połączenia**.
- b. Prawym przyciskiem myszy kliknij pozycję **Według grupy** i wybierz opcję **Nowa grupa połączeń z kluczem dynamicznym**.
- c. Na stronie **Ogólne** określ nazwę grupy. Na przykład L2TPDoCentrali.
- d. Wybierz opcję **Chroni lokalnie inicjowany tunel L2TP**.
- e. Jako rolę systemu wybierz opcję **Obydwa systemy to hosty**.
- f. Przejdź do strony **Strategia**. Z rozwijanej listy **Strategie danych** wybierz strategię danych utworzoną w punkcie 2, to jest **ZdalnyUzytkownikL2TP**.
- g. Wybierz opcję **Połączenie inicjowane przez system lokalny**, aby wskazać, że tylko serwer iSeries-A może inicjować połączenia z serwerem iSeries-B.
- h. Przejdź do strony **Połączenia**. Wybierz opcję **Generuj następującą regułę filtrowania strategii dla tej grupy**. Kliknij przycisk **Edytuj**, aby zdefiniować parametry filtra strategii.
- i. Na stronie **Filtr strategii - Adres lokalny** wybierz opcję **Identyfikator klucza** jako typ identyfikatora.
- j. Wybierz identyfikator klucza **ToJestIdKlucza**, zdefiniowany w strategii protokołu IKE.
- k. Przejdź do strony **Filtr strategii - Adresy zdalne**. Z rozwijanej listy **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
- l. W polu **Identyfikator** wpisz 205.13.237.6.
- m. Przejdź do strony **Filtr strategii - Usługi**. W polach **Port lokalny** i **Port zdalny** wpisz 1701. Port 1701 jest powszechnie używanym portem dla protokołu L2TP.
- n. Z rozwijanej listy **Protokół** wybierz pozycję **UDP**.
- o. Kliknij przycisk **OK**, aby powrócić do strony **Połączenia**.
- p. Przejdź do strony **Interfejsy**. Wybierz dowolną linię lub profil PPP, którego dotyczyć będzie ta grupa. Profil PPP dla tej grupy nie został jeszcze utworzony. Po jego utworzeniu w następnym kroku konieczna będzie edycja właściwości tej grupy, aby używała nowo utworzonego profilu.
- q. Kliknij przycisk **OK**, aby utworzyć grupę z kluczem dynamicznym L2TPDoCentrali.

Teraz trzeba dodać połączenie do utworzonej grupy.

### 5. Konfigurowanie połączenia z kluczem dynamicznym

- a. W interfejsie VPN rozwiń pozycję **Według grupy**. Zostanie wyświetlona lista wszystkich grup z kluczem dynamicznym zdefiniowanych na serwerze iSeries-A.
- b. Prawym przyciskiem myszy kliknij pozycję **L2TPDoCentrali** i wybierz opcję **Nowe połączenie z kluczem dynamicznym**.
- c. Na stronie **Ogólne** wpisz opcjonalny opis połączenia.
- d. Dla zdalnego serwera kluczy wybierz opcję **Adres IP wersja 4** jako typ identyfikatora.
- e. Z rozwijanej listy **Adres IP** wybierz pozycję 205.13.237.6.
- f. Anuluj wybór opcji **Uruchom na żądanie**.
- g. Przejdź do strony **Adresy lokalne**. Wybierz opcję **Identyfikator klucza** jako typ identyfikatora, a następnie wybierz pozycję **ToJestIdKlucza** z rozwijanej listy **Identyfikator**.
- h. Przejdź do strony **Adresy zdalne**. Jako typ identyfikatora wybierz **Adres IP wersja 4**.
- i. W polu **Identyfikator** wpisz 205.13.237.6.
- j. Przejdź do strony **Usługi**. W polach **Port lokalny** i **Port zdalny** wpisz 1701. Port 1701 jest powszechnie używanym portem dla protokołu L2TP.
- k. Z rozwijanej listy **Protokół** wybierz pozycję **UDP**.
- l. Kliknij przycisk **OK**, aby utworzyć połączenie z kluczem dynamicznym.

Konfigurowanie sieci VPN dla serwera iSeries-A zostało zakończone. Kolejnym krokiem jest skonfigurowanie profilu PPP dla serwera iSeries-A.

## **Krok 2: Konfigurowanie profilu połączenia PPP i linii wirtualnej na serwerze iSeries-A**

W tej sekcji opisano czynności, które należy wykonać w celu utworzenia profilu PPP dla serwera iSeries-A. Z profilem PPP nie jest powiązana żadna linia fizyczna, używa on linii wirtualnej. Dzieje się tak dlatego, że ruch PPP jest przesyłany tunelem PPP przez tunel L2TP, a sieci VPN chronią tunele L2TP.

Aby utworzyć profil połączenia PPP dla serwera iSeries-A, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję iSeries-A —>**Sieć** —>**Usługi zdalnego dostępu**.
2. Prawym przyciskiem myszy kliknij pozycję **Profile połączenia nadawcy** i wybierz opcję **Nowy profil**.
3. Na stronie **Konfiguracja** wybierz opcję **PPP** jako typ protokołu.
4. Jako tryb wybierz **L2TP (linia wirtualna)**.
5. Wybierz **Inicjator na żądanie (tunel dobrowolny)** z rozwijanej listy **Tryb pracy**.
6. Kliknij przycisk **OK**, aby przejść do strony właściwości profili PPP.
7. Na stronie **Ogólne** wpisz nazwę identyfikującą typ połączenia i jego miejsce docelowe. W tym wypadku wpisz DoCentrali. Wpisana nazwa nie może mieć więcej niż 10 znaków.
8. (opcjonalnie) Wprowadź opis tego profilu.
9. Przejdź do strony **Połączenie**.
10. Z rozwijanej listy w polu **Nazwa linia pojedyncza** wybierz pozycję **DoCentrali**. Należy pamiętać, że z tą linią nie jest powiązany żaden interfejs fizyczny. Linia wirtualna opisuje różne cechy tego profilu PPP; na przykład maksymalną wielkość ramki, informacje o uwierzytelnianiu, nazwę lokalnego hosta i tym podobne. Zostanie otworzone okno dialogowe **Właściwości linii L2TP**.
11. Na stronie **Ogólne** wpisz opis linii wirtualnej.
12. Przejdź do strony **Uwierzytelnianie**.
13. W polu **Nazwa użytkownika** wpisz nazwę hosta lokalnego serwera kluczy, czyli iSeries-A.
14. Kliknij przycisk **OK**, aby zapisać opis nowej linii wirtualnej i powrócić do strony **Połączenia**.
15. W polu **Adres odległego punktu końcowego tunelu** wpisz 205.13.237.6.
16. Wybierz opcję **Wymagana ochrona IPSec**, a następnie wybierz utworzoną w punkcie 1 grupę z kluczem dynamicznym L2TPDoCentrali z rozwijanej listy **Nazwa grupy połączenia**.
17. Przejdź do strony **Ustawienia TCP/IP**.
18. W sekcji **Lokalny adres IP** wybierz opcję **Przypisany przez system zdalny**.
19. W sekcji **Zdalny adres IP** wybierz opcję **Użyj stałego adresu IP**. Wpisz 10.6.11.1, czyli adres IP zdalnego systemu w jego podsieci.
20. W sekcji routingu wybierz opcję **Definiuj dodatkowe trasy statyczne** i kliknij przycisk **Trasy**. Jeśli w profilu PPP nie ma żadnych informacji o routingu, serwer iSeries-A nie będzie mógł łączyć się z żadnym innym systemem w podsieci 10.6.0.0 oprócz odległego punktu końcowego tunelu.
21. Kliknij przycisk **Dodaj**, aby dodać wpis trasy statycznej.
22. Wpisz adres 10.6.0.0 i maskę podsieci 255.255.0.0, aby cały ruch z adresów 10.6.\*.\* był kierowany przez tunel L2TP.
23. Kliknij przycisk **OK**, aby dodać trasę statyczną.
24. Kliknij przycisk **OK**, aby zamknąć okno dialogowe Routing.
25. Przejdź do strony **Uwierzytelnianie**, aby ustawić nazwę i hasło użytkownika dla tego profilu PPP.
26. W sekcji identyfikującej system lokalny wybierz opcję **Pozwól systemowi zdalnemu weryfikować tożsamość tego systemu**.
27. W sekcji **Używany protokół uwierzytelniania** wybierz pozycję **Wymaga szyfrowanego hasła (CHAP-MD5)**.
28. Wpisz nazwę użytkownika serwera iSeries-A i hasło.
29. Kliknij przycisk **OK**, aby zapisać profil PPP.

### Krok 3: Wprowadzenie grupy z kluczem dynamicznym L2TPDoCentrali do profilu PPP DoCentrali

Po skonfigurowaniu profilu PPP należy powrócić do utworzonej wcześniej grupy z kluczem dynamicznym L2TPDoCentrali i powiązać ją z profilem PPP. W tym celu wykonaj następujące czynności:

1. Otwórz interfejs VPN, a następnie rozwiń pozycję **Połączenia chronione**—>**Według grup**.
2. Prawym przyciskiem myszy kliknij grupę L2TPDoCentrali i wybierz opcję **Właściwości**.
3. Przejdź do strony **Interfejsy** i wybierz opcję **Zastosuj tę grupę** dla utworzonego w punkcie 2 profilu DoCentrali.
4. Kliknij przycisk **OK**, aby zastosować grupę L2TPDoCentrali do profilu PPP DoCentrali.

### Krok 4: Konfigurowanie sieci VPN dla serwera iSeries-B

Należy powtórzyć te same czynności, które wykonano podczas konfigurowania serwera iSeries-A, zmieniając odpowiednio adresy IP i identyfikatory. Przed rozpoczęciem należy zapoznać się z poniższymi uwagami:

- Przypisz zdalnemu serwerowi kluczy identyfikator klucza określony dla lokalnego serwera kluczy na serwerze iSeries-A. Na przykład ToJestIdKlucza.
- Użyj *dokładnie* tego samego wstępnego klucza współużytkowanego.
- Sprawdź, czy transformacje są zgodne z tymi, które skonfigurowano na serwerze iSeries-A; jeśli nie, nie będzie można nawiązać połączenia.
- Nie wybieraj opcji **Ochrona lokalnie inicjowanego tunelu L2TP** na stronie **Ogólne** grupy z kluczem dynamicznym.
- Zdalny system inicjuje połączenie.
- Zaznacz uruchamianie połączenia na żądanie.

### Krok 5: Konfigurowanie profilu połączenia PPP i linii wirtualnej na serwerze iSeries-B

Aby utworzyć profil połączenia PPP dla serwera iSeries-B, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję iSeries-B —>**Sieć** —>**Usługi zdalnego dostępu**.
2. Prawym przyciskiem myszy kliknij pozycję **Profil połączenia odbiorcy** i wybierz opcję **Nowy profil**.
3. Na stronie **Konfiguracja** wybierz opcję **PPP** jako typ protokołu.
4. Jako tryb wybierz **L2TP (linia wirtualna)**.
5. Z rozwijanej listy **Tryb pracy** wybierz **Terminator (serwer sieciowy)**.
6. Kliknij przycisk **OK**, aby przejść do stron właściwości profili PPP.
7. Na stronie **Ogólne** wpisz nazwę identyfikującą typ połączenia i jego miejsce docelowe. W tym wypadku wpisz DoOddziału. Wpisana nazwa nie może mieć więcej niż 10 znaków.
8. (opcjonalnie) Wprowadź opis tego profilu.
9. Przejdź do strony **Połączenie**.
10. Wpisz adres IP lokalnego punktu końcowego tunelu, czyli 205.13.237.6.
11. Z rozwijanej listy w polu **Nazwa linii wirtualnej** wybierz pozycję **DoOddziału**. Należy pamiętać, że z tą linią nie jest powiązany żaden interfejs fizyczny. Linia wirtualna opisuje różne cechy tego profilu PPP; na przykład maksymalną wielkość ramki, informacje o uwierzytelnianiu, nazwę lokalnego hosta i tym podobne. Zostanie otworzone okno dialogowe **Właściwości linii L2TP**.
12. Na stronie **Ogólne** wpisz opis linii wirtualnej.
13. Przejdź do strony **Uwierzytelnianie**.
14. W polu **Nazwa hosta lokalnego** wpisz nazwę hosta lokalnego serwera kluczy, czyli iSeries-B.
15. Kliknij przycisk **OK**, aby zapisać opis nowej linii wirtualnej i powrócić do strony **Połączenia**.
16. Przejdź do strony **Ustawienia TCP/IP**.
17. W polu **Lokalny adres IP** wpisz stały adres IP systemu lokalnego, czyli 10.6.11.1.
18. W polu **Zdalny adres IP** wybierz opcję **Pula adresów** jako sposób przypisywania adresów. Wpisz adres początkowy, a następnie określ liczbę adresów, które mogą być przypisane systemowi zdalnemu.
19. Wybierz opcję **Pozwól zdalnemu systemowi na dostęp do innych sieci (przekazywanie IP)**.



20. Przejdź do strony **Uwierzytelnianie**, aby ustawić nazwę i hasło użytkownika dla tego profilu PPP.
21. W sekcji identyfikującej system lokalny wybierz opcję **Pozwól systemowi zdalnemu weryfikować tożsamość tego systemu**. Spowoduje to otwarcie okna dialogowego **Identyfikacja systemu lokalnego**.
22. W sekcji **Używany protokół uwierzytelniania** wybierz pozycję **Wymaga szyfrowanego hasła (CHAP-MD5)**.
23. Wpisz nazwę użytkownika serwera iSeries-B i hasło.
24. Kliknij przycisk **OK**, aby zapisać profil PPP.

#### Krok 6: Uaktywnienie reguł pakietów

Ustawienia sieci VPN spowodują automatyczne utworzenie reguł pakietów wymaganych do poprawnego działania tego połączenia. Zanim jednak będzie można uruchomić połączenie VPN, należy je uaktywnić na obydwu serwerach. W tym celu wykonaj następujące czynności na serwerze iSeries-A:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** —>**Sieć** —>**Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Uaktywnij**. Spowoduje to otwarcie okna dialogowego **Uaktywnij reguły pakietów**.
3. Wybierz uaktywnienie wyłącznie wygenerowanych reguł VPN, wyłącznie wybranego pliku lub zarówno wygenerowanych reguł VPN, jak i wybranego pliku. Można wybrać ostatnią opcję, aby na przykład wymusić na interfejsie różne reguły typu PERMIT i DENY, oprócz wygenerowanych reguł VPN.
4. Wybierz interfejs, dla którego chcesz uaktywnić reguły. W tym wypadku wybierz opcję **Wszystkie interfejsy**.
5. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić zamiar weryfikacji i uaktywnienia reguł dla określonych interfejsów. Po kliknięciu przycisku OK system sprawdzi składniową i semantyczną poprawność reguł oraz wyświetli wyniki w oknie komunikatu u dołu edytora. W wypadku komunikatów o błędach dotyczących określonego pliku i numeru wiersza można kliknąć dany komunikat prawym przyciskiem myszy i wybrać opcję **Przejdź do wiersza**, aby wyróżnić błąd w pliku.
6. Powtórz powyższe czynności, aby uaktywnić reguły pakietów na serwerze iSeries-B.

#### Krok 7: Uruchomienie połączenia

Ostatni krok polega na uruchomieniu połączenia. Aby można było zainicjować połączenie L2TP, konieczne jest włączenie odpowiedzi terminatora L2TP na żądania inicjatora. Po sprawdzeniu, czy wszystkie wymagane usługi zostały uruchomione, należy uruchomić połączenie PPP po stronie terminatora. Poniżej opisano czynności niezbędne do uruchomienia połączenia PPP na serwerze iSeries-B:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-B** —>**Sieć** —>**Usługi zdalnego dostępu**.
2. Kliknij pozycję **Profile połączenia odbiorcy**, aby wyświetlić listę profili respondenta w prawej części okna.
3. Kliknij prawym przyciskiem myszy pozycję **DoOddziału** i wybierz opcję **Uruchom**. Po uruchomieniu profilu połączenia zawartość okna zostanie odświeżona i zostanie w nim wyświetlony status połączenia: **Oczekiwanie na żądania połączenia**. Serwer iSeries-A będzie mógł teraz odpowiadać na żądania połączenia L2TP z serwera iSeries-B.

Aby uruchomić połączenie L2TP na serwerze iSeries-A, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję **iSeries-A** —>**Sieć** —>**Usługi zdalnego dostępu**.
2. Kliknij pozycję **Profile połączenia inicjatora**, aby wyświetlić listę profili inicjatora w prawej części okna.
3. Kliknij prawym przyciskiem myszy pozycję **DoCentrali** i wybierz opcję **Uruchom**. Po uruchomieniu profilu połączenia zawartość okna zostanie odświeżona i zostanie w niej wyświetlony status połączenia: **Tworzenie tunelu L2TP**.
4. Naciśnij klawisz F5, aby odświeżyć ekran. Jeśli tunel L2TP został uruchomiony pomyślnie, status połączenia zmieni się na **Połączenia aktywne**.

## Scenariusz VPN: Wykorzystanie translacji adresów sieciowych na potrzeby sieci VPN

W tym scenariuszu za przykład posłuży sieć niewielkiej firmy produkcyjnej z Poznania. Jeden z kontrahentów tej firmy, dostawca podzespołów z Gdańska, chce wykorzystać Internet do współpracy z tą firmą. Dla firmy produkcyjnej

ogromne ma dostęp do określonych części w wymaganych ilościach i w zaplanowanym czasie, dlatego dostawca musi na bieżąco znać stan zapasów producenta i jego harmonogramy produkcji. Obecnie problem ten jest rozwiązywany w sposób tradycyjny (telefonicznie, faksem), co jednak jest czasochłonne, kosztowne, a niekiedy może prowadzić do błędów, dlatego obie firmy są bardzo zainteresowane znalezieniem innych rozwiązań.

Ze względu na poufność i szybkie zmiany informacji wymienianych przez kontrahentów, zdecydowano się na utworzenie sieci VPN łączącej sieć dostawcy z siecią producenta. Aby dodatkowo zwiększyć ochronę struktury sieci firmowej, podjęto decyzję o ukryciu prywatnego adresu IP serwera iSeries<sup>(TM)</sup>, będącego hostem aplikacji, do których dostęp ma dostawca. Powstaje pytanie: jak wdrożyć ten plan?

Aby go zrealizować, należy wykorzystać moduł OS/400<sup>(R)</sup> VPN. Rozwiązanie to posłuży nie tylko do zdefiniowania połączeń bramy VPN w sieci firmy produkcyjnej, ale także umożliwi translację adresów sieciowych, która ukryje adresy w sieci prywatnej. W przeciwieństwie do konwencjonalnej translacji adresów sieciowych (NAT), która zmienia adresy IP w powiązaniach Security Association (SA) niezbędnych do działania sieci VPN, translacja NAT w sieci VPN odbywa się przed sprawdzeniem poprawności powiązania SA przez przypisanie adresu do połączenia przy jego uruchamianiu.

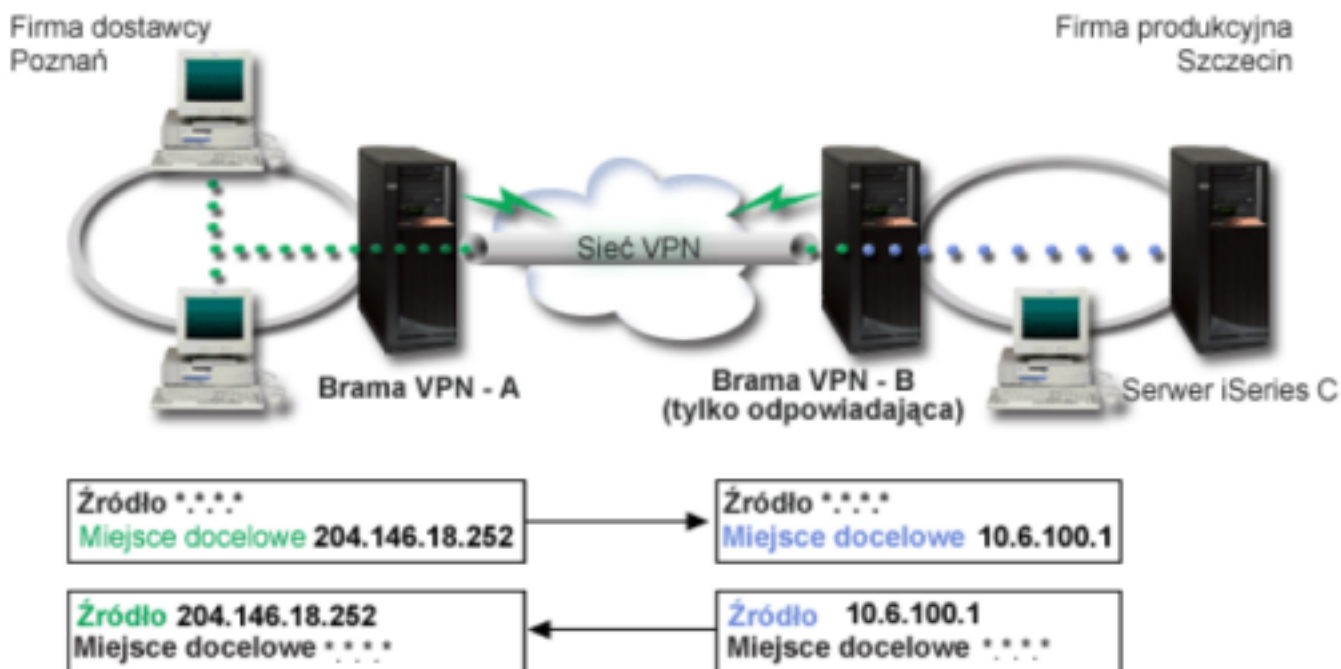
### Cele

Celem tego scenariusza jest:

- umożliwienie wszystkim klientom w sieci dostawcy dostępu do jednego hosta iSeries w sieci producenta przez połączenie VPN między bramami,
- ukrycie prywatnego adresu IP hosta iSeries w sieci producenta, poprzez jego translację na publiczny adres IP za pomocą funkcji translacji adresów sieciowych dla sieci VPN (VPN NAT).

### Szczegóły

Poniższy schemat przedstawia sieć dostawcy i sieć producenta:



- Brama VPN A jest skonfigurowana tak, że to zawsze ona inicjuje połączenia z bramą VPN B.
- Brama VPN A definiuje docelowy punkt końcowy dla połączenia jako 204.146.18.252 (publiczny adres przypisany serwerowi iSeries-C).
- Prywatny adres IP serwera iSeries-C w sieci producenta to 10.6.100.1.
- W lokalnej puli usług bramy VPN B dla prywatnego adresu serwera iSeries-C 10.6.100.1 zdefiniowano publiczny adres IP 204.146.18.252.

- Dla przychodzących datagramów brama VPN B dokonuje translacji publicznego adresu serwera iSeries-C na jego adres prywatny 10.6.100.1. Dla datagramów wychodzących brama VPN B dokonuje translacji z adresu 10.6.100.1 z powrotem na publiczny adres serwera iSeries-C, czyli 204.146.18.252. Dla klientów w sieci dostawcy serwer iSeries-C ma zawsze adres IP 204.146.18.252. Nigdy nie dowiedzą się oni o translacji tego adresu.

### Zadania konfiguracyjne

Aby skonfigurować połączenie opisane w tym scenariuszu, wykonaj następujące zadania konfiguracyjne:

1. Skonfiguruj podstawowe połączenie VPN pomiędzy **Bramą VPN A** i **Bramą VPN B**.
2. Zdefiniuj lokalną pulę usług na **Bramie VPN B**, aby ukryć prywatny adres serwera **iSeries-C** za publicznym identyfikatorem 204.146.18.252.
3. Skonfiguruj na **Bramie VPN B** translację lokalnego adresu, używając adresów z lokalnej puli usług.

---

## Koncepcje sieci VPN

Do zabezpieczenia przesyłanych danych w technologii wirtualnych sieci prywatnych (VPN) wykorzystuje się kilka ważnych protokołów TCP/IP. Aby lepiej zrozumieć sposób działania połączenia VPN, należy poznać te protokoły oraz sposób ich wykorzystania w produkcie OS/400<sup>(R)</sup> VPN, czytając poświęcone im sekcje:

- “Protokoły IP Security (IPSec)”  
Protokół IPSec stanowi stabilną i trwałą bazę bezpieczeństwa warstwy sieci.
- “Zarządzanie kluczami” na stronie 24  
W dynamicznych połączeniach VPN wprowadza się dodatkowe zabezpieczenia łączności, wykorzystując protokół Internet Key Exchange (IKE) do zarządzania kluczami. Protokół IKE umożliwia serwerom VPN na obu końcach połączenia negocjowanie nowych kluczy w określonych odstępach czasu.
- “Protokół Layer 2 Tunnel Protocol (L2TP)” na stronie 26  
Jeśli planuje się wykorzystanie połączenia VPN do ochrony komunikacji pomiędzy lokalną siecią a zdalnymi klientami, należy także znać podstawy protokołu L2TP.
- “Translacja adresów sieciowych dla sieci VPN” na stronie 26  
Produkt OS/400 VPN udostępnia możliwości translacji adresów sieciowych zwanej VPN NAT. Translacja VPN NAT różni się do tradycyjnej translacji NAT tym, że odbywa się przed zastosowaniem protokołów IKE i IPSec. Więcej na ten temat można dowiedzieć się z sekcji poświęconej translacji VPN NAT.
- “Zgodność translacji NAT i protokołów IPSec” na stronie 27  
Hermetyzacja UDP umożliwia przesyłanie ruchu IPSec przez konwencjonalne urządzenie NAT. W tej sekcji znajduje się więcej informacji dotyczących istoty i sposobu wykorzystania hermetyzacji UDP na potrzeby połączeń VPN.
- “Protokół IP Compression (IPComp)” na stronie 29  
Protokół IPComp pozwala zredukować wielkość datagramów IP poprzez ich kompresję, co prowadzi do zwiększenia wydajności łącza komunikacyjnego pomiędzy dwoma stronami połączenia VPN.
- “Sieci VPN i filtrowanie IP” na stronie 29  
Zagadnienia filtrowania IP i sieci VPN są ze sobą ściśle związane. W rzeczywistości większość połączeń VPN do prawidłowej pracy wymaga reguł filtrowania. W tej sekcji zamieszczono informacje o wymaganiach filtrów VPN, a także o innych koncepcjach dotyczących filtrowania związanych z sieciami VPN.

## Protokoły IP Security (IPSec)

Protokół IPSec stanowi stabilną i trwałą bazę bezpieczeństwa warstwy sieci. Obsługuje on wszystkie używane współcześnie algorytmy szyfrujące i może także dostosować się do nowszych, silniejszych algorytmów, które pojawiają się w przyszłości. Protokoły IPSec stanowią odpowiedź na poniższe główne zagadnienia dotyczące bezpieczeństwa:

### Uwierzytelnianie pochodzenia danych

Sprawdzanie, czy każdy datagram pochodzi od podanego nadawcy.

### Integralność danych

Sprawdzenie, czy zawartość datagramu nie została zmieniona podczas przesyłania - umyślnie lub na skutek przypadkowych błędów.

### Poufność danych

Ukrywanie treści wiadomości, zwykle za pomocą szyfrowania.

## Ochrona odpowiedzi

Uniemożliwienie napastnikowi przechwycenia datagramu i późniejszego wykorzystania go.

### Automatyczne zarządzanie kluczami szyfrującymi i powiązaniem Security Association


Umożliwienie użycia strategii VPN w rozbudowanej sieci z minimalnymi wymaganiami w zakresie ręcznego konfigurowania ustawień lub nawet bez ingerencji użytkownika.

Do ochrony danych przesyłanych przez połączenie VPN wykorzystuje się dwa protokoły IPsec: Authentication Header (AH) i Encapsulating Security Payload (ESP). Innym elementem związanym z uaktywnianiem IPsec jest protokół Internet Key Exchange (IKE), czyli zarządzanie kluczami. Podczas gdy protokoły IPsec szyfrują przesyłane dane, protokół IKE obsługuje zautomatyzowane negocjacje powiązań Security Association (SA) oraz automatyczne generowanie i odświeżanie kluczy szyfrujących.

Główne protokoły IPsec to:

- “Protokół Authentication Header”
- “Protokół Encapsulating Security Payload” na stronie 23
- “Kombinacja protokołów AH i ESP” na stronie 24
- “Zarządzanie kluczami” na stronie 24

Formalna definicja protokołów IPsec została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comment (RFC) 2401 zatytułowanym *Security Architecture for the Internet*

*Protocol*. Dokument ten jest dostępny w serwisie internetowym: <http://www.rfc-editor.org> .

## Protokół Authentication Header

Protokół Authentication Header (AH) zapewnia uwierzytelnianie pochodzenia danych, ich integralność oraz ochronę odpowiedzi. Nie gwarantuje on jednak poufności danych, ponieważ przesyła je w postaci jawnej.

Integralność danych w protokole AH jest realizowana za pomocą sumy kontrolnej generowanej przez kody uwierzytelniania komunikatu, na przykład MD5. Do uwierzytelniania pochodzenia danych protokół AH używa tajnego wstępnego klucza współużytkowanego w swoim algorytmie uwierzytelniania. Do ochrony odpowiedzi protokół AH używa pola z numerem kolejnym w nagłówku AH. Warto zauważyć, że te trzy odrębne funkcje są często łączone i określane wspólnym terminem **uwierzytelnianie**. Mówiąc krótko, protokół AH gwarantuje, że przesyłane dane nie uległy po drodze żadnej manipulacji.

Mimo że protokół AH uwierzytelnia maksymalną możliwą część datagramu IP, odbiorca nie może przewidzieć wartości niektórych pól z nagłówka IP. Tym samym protokół AH nie może chronić tych pól, znanych jako pola **zmienne (mutable)**. Protokół ten zawsze jednak chroni dane właściwe w pakiecie IP.

Formalna definicja protokołu AH została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comment (RFC) 2402 zatytułowanym *IP Authentication Header*. Dokument ten jest

dostępny w serwisie internetowym: <http://www.rfc-editor.org> .

### Metody korzystania z protokołu AH

Protokół AH można stosować na dwa sposoby: w trybie transportowym lub w trybie tunelowym. W trybie transportowym nagłówek IP datagramu jest nagłówkiem zewnętrznym, po którym następuje nagłówek AH, a potem dane właściwe datagramu. Protokół AH uwierzytelnia cały datagram z wyjątkiem pól zmiennych. Jednak informacje zawarte w datagramie są transportowane w postaci jawnej, co stwarza ryzyko ich przechwycenia. Obciążenie związane z trybem transportowym jest mniejsze niż w przypadku trybu tunelowego, jednak ochrona w tym trybie jest słabsza niż w trybie tunelowym.

W trybie tunelowym tworzony jest nowy nagłówek IP, który jest używany jako zewnętrzny nagłówek IP datagramu. Nagłówek AH jest umieszczany po nowym nagłówku IP. Na końcu znajduje się oryginalny datagram (zarówno nagłówek IP, jak i pierwotne dane właściwe). Protokół AH uwierzytelnia cały datagram, co oznacza, że zdalny system może wykryć, czy datagram został zmieniony podczas przesyłania.

Jeśli jeden z punktów końcowych Security Association jest bramą, należy korzystać z trybu tunelowego. W trybie tym adresy źródłowy i docelowy w zewnętrznym nagłówku IP nie muszą być takie same, jak w oryginalnym nagłówku IP. Na przykład dwie bramy ochrony mogą wykorzystywać tunel AH do uwierzytelniania całego ruchu pomiędzy sieciami, które łączą ze sobą. W rzeczywistości jest to bardzo typowa konfiguracja.

Główną zaletą trybu tunelowego jest to, że całkowicie chroni on zahermetyzowany datagram IP. Ponadto tryb tunelowy umożliwia wykorzystanie adresów prywatnych.

### **Dlaczego AH?**

W wielu przypadkach dane wymagają tylko uwierzytelnienia. Chociaż protokół "Protokół Encapsulating Security Payload" również może uwierzytelniać dane, jego zastosowanie znacznie wyraźniej odbija się na wydajności systemu niż w zastosowanie protokołu AH. Inną zaletą protokołu AH jest to, że uwierzytelnia on cały datagram. Jednakże protokół ESP nie uwierzytelnia zewnętrznego nagłówka IP ani żadnych innych danych, które występują przed nagłówkiem ESP.

Ponadto wdrożenie protokołu ESP wymaga silnych kluczy szyfrujących. Użycie takich kluczy jest w niektórych krajach ograniczone obowiązującymi przepisami; ograniczeniom tym nie podlega protokół AH i może być swobodnie stosowany na całym świecie.

### **Algorytmy używane przez protokół AH do ochrony informacji**

Protokół AH wykorzystuje algorytm znany pod nazwą **hashed message authentication codes (HMAC)**. W szczególności w sieciach VPN używany jest algorytm HMAC-MD5 lub HMAC-SHA. Oba algorytmy na podstawie danych wejściowych o zmiennej długości i tajnego klucza tworzą dane wyjściowe o stałej długości (zwane wartością mieszającą - hash value). Jeśli wartości mieszające obydwu wiadomości są zgodne, jest bardzo prawdopodobne, że wiadomości te są takie same. Zarówno algorytm MD5, jak i SHA kodują długość wiadomości w danych wyjściowych, ale algorytm SHA jest uważany za bezpieczniejszy, ponieważ tworzy dłuższe wartości mieszające.

Formalna definicja algorytmu HMAC-MD5 została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comments (RFC) 2085 zatytułowanym *HMAC-MD5 IP Authentication with replay prevention*. Formalna definicja algorytmu HMAC-SHA została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comments (RFC) 2404 zatytułowanym *The Use of HMAC-SHA-1-96 within ESP and AH*. Dokumenty te są dostępne w serwisie internetowym:

<http://www.rfc-editor.org>  .

### **Protokół Encapsulating Security Payload**

Protokół Encapsulating Security Payload (ESP) zapewnia poufność danych, a także opcjonalnie uwierzytelnianie pochodzenia danych, sprawdzanie integralności i ochronę odpowiedzi. Te same funkcje realizuje protokół "Protokół Authentication Header" na stronie 22, z tym że protokół ESP dodatkowo umożliwia szyfrowanie danych. Protokół ESP wymaga, aby obydwa komunikujące się ze sobą systemy używały wspólnego klucza do szyfrowania i deszyfrowania wymienianych danych.

W wypadku jednoczesnego zastosowania funkcji szyfrowania i uwierzytelniania, system odpowiadający najpierw uwierzytelnia pakiet, a następnie, jeśli pierwszy krok zakończy się powodzeniem, przystępuje do odszyfrowania treści pakietu. Konfiguracja tego typu redukuje obciążenie związane z przetwarzaniem oraz zmniejsza ryzyko ataków typu odmowa usługi (denial-of-service).

### **Dwie metody wykorzystania protokołu ESP**

Protokół ESP można stosować na dwa sposoby: w trybie transportowym lub w trybie tunelowym. W trybie transportowym nagłówek ESP występuje po nagłówku IP oryginalnego datagramu. Jeśli ten datagram ma już nagłówek IPSec, wówczas nagłówek ESP jest wstawiany przed nim. Etykieta końcowa ESP i opcjonalne dane uwierzytelniające są umieszczane po danych właściwych.

W trybie transportowym nagłówek IP nie jest uwierzytelniany ani szyfrowany, co może stworzyć ryzyko zmiany informacji adresowych podczas przesyłania datagramu. Obciążenie związane z trybem transportowym jest mniejsze niż



w przypadku trybu tunelowego, jednak ochrona w tym trybie jest słabsza niż w trybie tunelowym. W większości przypadków hosty korzystają z protokołu ESP w trybie transportowym.

W trybie tunelowym tworzony jest nowy nagłówek IP, który jest używany jako zewnętrzny nagłówek IP datagramu; po nim umieszczany jest nagłówek ESP a potem oryginalny datagram (zarówno nagłówek IP, jak i pierwotne dane właściwe). Etykieta końcowa ESP i opcjonalne dane uwierzytelniające są dołączane do danych właściwych. Jednoczesne zastosowanie szyfrowania i uwierzytelniania w protokole ESP zapewnia pełną ochronę oryginalnego datagramu, który stanowi dane właściwe nowego pakietu ESP. Jednak protokół ESP nie chroni nowego nagłówka IP. Bramy muszą korzystać z protokołu ESP w trybie tunelowym.

### **Algorytmy używane przez protokół ESP do ochrony informacji**

W protokole ESP wykorzystywany jest klucz symetryczny, za pomocą którego obie strony sesji komunikacyjnej szyfrują i deszyfrują przesyłane między sobą dane. Przed nawiązaniem bezpiecznej komunikacji nadawca i odbiorca muszą uzgodnić klucz. Produkt OS/400<sup>(R)</sup> VPN wykorzystuje do szyfrowania następujące algorytmy: Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4 lub Advanced Encryption Standard (AES).

Formalna definicja algorytmu DES została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comment (RFC) 1829 zatytułowanym *The ESP DES-CBC Transform*. Formalna definicja algorytmu 3DES została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comment (RFC) 1851 zatytułowanym *The ESP Triple DES Transform*. Te i inne dokumenty

RFC są dostępne w serwisie internetowym: <http://www.rfc-editor.org> .

Funkcje uwierzytelniania w protokole ESP są realizowane przy użyciu algorytmów HMAC-MD5 i HMAC-SHA. Oba algorytmy na podstawie danych wejściowych o zmiennej długości i tajnego klucza tworzą dane wyjściowe o stałej długości (zwane wartością mieszającą - hash value). Jeśli wartości mieszające obydwu wiadomości są zgodne, jest bardzo prawdopodobne, że wiadomości te są takie same. Zarówno algorytm MD5, jak i SHA kodują długość wiadomości w danych wyjściowych, ale algorytm SHA jest uważany za bezpieczniejszy, ponieważ tworzy dłuższe wartości mieszające.

Formalna definicja algorytmu HMAC-MD5 została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comments (RFC) 2085 zatytułowanym *HMAC-MD5 IP Authentication with replay prevention*. Formalna definicja algorytmu HMAC-SHA została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comments (RFC) 2404 zatytułowanym *The Use of HMAC-SHA-1-96 within ESP and AH*. Te i inne dokumenty RFC są dostępne w serwisie

internetowym: <http://www.rfc-editor.org> .

### **Kombinacja protokołów AH i ESP**

Sieci VPN umożliwiają jednoczesne stosowanie protokołów AH i ESP dla połączeń między hostami w trybie transportowym. Połączenie tych protokołów zapewnia pełną ochronę całego datagramu IP. Mimo że rozwiązanie to oferuje większe bezpieczeństwo, obciążenie związane z przetwarzaniem może spowodować, że koszt tego rozwiązania będzie większy niż uzyskane dzięki niemu korzyści.

### **Zarządzanie kluczami**

Po pomyślnym zakończeniu negocjacji serwery VPN zawsze odnawiają klucze chroniące połączenie, utrudniając tym samym osobom niepowołanym przechwycenie informacji przesyłanych tym połączeniem. Jeśli dodatkowo używane jest zabezpieczenie typu Perfect Forward Secrecy (PFS), osoba taka nie będzie w stanie obliczyć przyszłych wartości kluczy na podstawie wartości wcześniejszych.

VPN Key Manager to opracowana przez firmę IBM<sup>(TM)</sup> implementacja protokołu Internet Key Exchange (IKE). Menedżer kluczy obsługuje automatyczne negocjowanie Security Association (SA), a także automatyczne generowanie i odświeżanie kluczy szyfrujących.

**Security Association (SA)** zawiera informacje niezbędne do wykorzystania protokołów IPSec. Powiązanie SA identyfikuje na przykład typy algorytmów, długości i terminy ważności kluczy, uczestników połączenia i tryby hermetyzacji.

Klucze szyfrujące, jak sama nazwa wskazuje, chronią informacje, umożliwiając im bezpieczne dotarcie do miejsca docelowego.

**Uwaga:** O nawiązaniu bezpiecznego prywatnego połączenia decyduje przede wszystkim ochrona podczas generowania kluczy. Przechwycenie kluczy przez osoby nieupoważnione spowoduje, że wszystkie wysiłki związane z uwierzytelnianiem i szyfrowaniem pójdą na marne.

### Fazy zarządzania kluczami

W opisywanej implementacji VPN Key Manager działa w dwóch fazach.

#### Faza 1

W fazie 1. uzgadniany jest nadrzędny klucz tajny, na podstawie którego tworzone są klucze szyfrujące używane do ochrony danych użytkowników. Dzieje się to także wtedy, kiedy jeszcze nie skonfigurowano żadnych zabezpieczeń pomiędzy obydwoma punktami końcowymi. Do uwierzytelnienia fazy 1. negocjacji oraz do uzgodnienia kluczy zabezpieczających komunikaty IKE przesyłane w fazie 2. negocjacji, w sieci VPN używany jest albo podpis RSA albo wstępne klucze współużytkowane.

*Wstępny klucz współużytkowany* to nietrywialny łańcuch o długości do 128 znaków. Klucz ten musi zostać uzgodniony przez obydwie końce połączenia. Zaletą wstępnych kluczy współużytkowanych jest ich prostota, wadą jest to, że przed negocjacjami IKE należy je przesłać poza połączeniem, na przykład przekazać telefonicznie lub pocztą elektroniczną. Wstępny klucz współużytkowany należy traktować tak, jak hasło.

Uwierzytelnianie za pomocą *podpisu RSA* zapewnia większe bezpieczeństwo niż wstępne klucze współużytkowane, ponieważ w tym trybie używane są certyfikaty cyfrowe. Certyfikaty takie należy skonfigurować za pomocą programu Menedżer certyfikatów cyfrowych (5722-SS1 opcja 34). Ponadto podpis RSA jest wymagany do współdziałania niektórych rozwiązań dla sieci VPN. Na przykład implementacja VPN w Windows<sup>(R)</sup> 2000 wykorzystuje podpis RSA jako domyślną metodę uwierzytelniania. Należy zaznaczyć, że podpis RSA zapewnia znacznie większą skalowalność niż wstępne klucze współużytkowane. Certyfikaty używane do uwierzytelniania muszą pochodzić z ośrodka certyfikacji, który obydwie serwery uznają za zaufany.

#### Faza 2

Podczas fazy 2. negocjowane są powiązania Security Association i klucze, które będą chronić rzeczywistą wymianę danych aplikacji. Należy pamiętać, że jak dotąd żadne dane aplikacji nie zostały przesłane. Faza 1. negocjacji służy do zabezpieczenia komunikatów IKE wymienianych w fazie 2.

Po zakończeniu fazy 2. negocjacji serwer VPN nawiązuje bezpieczne, dynamiczne połączenie sieciowe pomiędzy dwoma punktami końcowymi zdefiniowanymi wcześniej dla tego połączenia. Stopień ochrony i wydajności wszystkich danych przesyłanych połączeniem VPN zostaje uzgodniony przez obydwie serwery kluczy podczas fazy 1. i 2. negocjacji.

W ogólności faza 1. negocjacji odbywa się raz dziennie, natomiast faza 2. negocjacji jest odświeżana co 60 minut lub nawet co 5 minut. Częstsze odświeżanie zwiększa bezpieczeństwo danych, ale obniża wydajność systemu. Do ochrony najcenniejszych danych należy używać kluczy z krótszym okresem ważności.

Podczas tworzenia dynamicznego połączenia VPN w programie iSeries<sup>(TM)</sup> Navigator konieczne jest “Konfigurowanie strategii protokołu Internet Key Exchange (IKE)” na stronie 38, aby umożliwić fazę 1. negocjacji, “Konfigurowanie strategii danych” na stronie 39, która określi przebieg fazy 2. negocjacji. Opcjonalnie można do tego celu użyć Kreatora nowego połączenia. Kreator automatycznie utworzy obiekty konfiguracyjne wymagane przez sieć VPN do prawidłowej pracy, w tym strategię IKE i strategię danych.

### Zalecane lektury

Aby dowiedzieć się więcej o protokole Internet Key Exchange (IKE) oraz o zarządzaniu kluczami, zapoznaj się z następującymi dokumentami RFC opublikowanymi przez grupę wykonawczą IETF (Internet Engineering Task Force):

- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*

Dokumenty te są dostępne w serwisie internetowym: <http://www.rfc-editor.org> .

## Protokół Layer 2 Tunnel Protocol (L2TP)

Połączenia w protokole Layer 2 Tunnel Protocol (L2TP), zwane również liniami wirtualnymi, stanowią dla zdalnych użytkowników ekonomiczny sposób dostępu i umożliwiają serwerom sieci korporacyjnych obsługę adresów IP przypisanych tym użytkownikom. Ponadto połączenia L2TP używane wraz z protokołami IPSec zapewniają bezpieczny dostęp do systemów i sieci.

Protokół L2TP obsługuje tunele w dwóch trybach: dobrowolnym i przymusowym. Główną różnicę pomiędzy tymi dwoma trybami tuneli stanowią punkty końcowe. Tunel dobrowolny kończy się u zdalnego klienta, podczas gdy tunel przymusowy kończy się u dostawcy ISP.

W przypadku **tunelu przymusowego** L2TP, zdalny host inicjuje połączenie ze swoim dostawcą ISP (Internet Service Provider). Następnie dostawca ISP nawiązuje połączenie L2TP pomiędzy zdalnym użytkownikiem a siecią korporacyjną. Pomimo tego, że połączenie jest nawiązywane przez dostawcę ISP, to użytkownik decyduje, jak zabezpieczyć ruch przy użyciu mechanizmów sieci VPN. Dla tuneli przymusowych dostawca ISP musi obsługiwać protokół L2TP.

W przypadku **dobrowolnego tunelu** L2TP, połączenie jest tworzone przez zdalnego użytkownika, najczęściej za pomocą klienta tunelowania L2TP. W rezultacie zdalny użytkownik wysyła pakiety L2TP do swojego dostawcy ISP, który przekazuje je do sieci korporacyjnej. Dla tuneli dobrowolnych dostawca ISP nie musi obsługiwać protokołu L2TP. W scenariuszu *“Scenariusz VPN: Ochrona dobrowolnego tunelu L2TP za pomocą protokołu IPSec”* na stronie 13 przedstawiono przykład konfigurowania serwera iSeries<sup>(TM)</sup> w biurze oddziału do połączeń z siecią przedsiębiorstwa poprzez bramę iSeries z tunelem L2TP zabezpieczonym mechanizmami sieci VPN.

➤ Dostępna jest prezentacja wizualna przedstawiająca dobrowolne tunele L2TP zabezpieczane protokołem IPSec.

Wymaga ona modułu dodatkowego Flash . Można również obejrzeć wersję HTML tej prezentacji. ⏪

Protokół L2TP jest w rzeczywistości odmianą protokołu hermetyzacji IP. Tunel L2TP jest tworzony przez wstawienie ramki L2TP wewnątrz pakietu protokołu User Datagram Protocol (UDP), który z kolei znajduje się wewnątrz pakietu IP. Adresy źródłowy i docelowy tego pakietu IP definiują punkty końcowe połączenia. Ponieważ zewnętrznym protokołem hermetyzującym jest IP, można zastosować protokoły IPSec do złożonego pakietu IP. Pozwoli to zabezpieczyć dane przesyłane tunelem L2TP. W prosty sposób można zastosować protokoły Authentication Header (AH), Encapsulated Security Payload (ESP) oraz Internet Key Exchange (IKE).

Należy zapoznać się z tematem Scenariusz: Konfigurowanie zdalnego połączenia modemowego z użyciem protokołu PPP, na przykład w jaki sposób używany jest L2TP podczas połączenia IBM<sup>(R)</sup> przez połączenie uniwersalne.

## Translacja adresów sieciowych dla sieci VPN

Translacja adresów sieciowych (NAT) polega na przekształcaniu prywatnych adresów IP w adresy publiczne. Pozwala to oszczędzać cenne adresy publiczne i jednocześnie umożliwia hostom z sieci lokalnej dostęp do usług i zdalnych hostów poprzez Internet (lub inną sieć publiczną).

Ponadto jeśli używane byłyby prywatne adresy IP, mogłoby dochodzić do kolizji z podobnymi adresami IP pakietów przychodzących. Na przykład zachodzi potrzeba komunikowania się z inną siecią, ale obydwie sieci korzystają z adresów klasy 10.\*.\*.\*, co powoduje kolizję adresów i porzucenie wszystkich pakietów. Zastosowanie translacji NAT



do adresów wychodzących może stanowić rozwiązanie tego problemu. Jeśli jednak ruch danych jest chroniony przez mechanizmy sieci VPN, konwencjonalna translacja NAT nie sprawdzi się, ponieważ zmienia ona adresy IP w powiązaniach Security Association (SA) wymaganych do funkcjonowania sieci VPN. Aby uniknąć tego problemu, rozwiązanie VPN oferuje własną wersję translacji NAT, zwaną VPN NAT. Translacja VPN NAT odbywa się przed sprawdzeniem poprawności powiązań SA poprzez przypisanie adresu do połączenia przy jego uruchamianiu. Adres pozostaje powiązany z połączeniem, aż do jego usunięcia.

**Uwaga:** Protokół FTP na razie nie obsługuje translacji VPN NAT.

### **Jak korzystać z translacji VPN NAT**

Istnieją dwa różne typy translacji VPN NAT, spośród których należy wybrać odpowiedni do indywidualnych wymagań. Są to:

#### **Translacja VPN NAT zapobiegająca konfliktom adresów IP**

Ten rodzaj translacji VPN NAT pozwala uniknąć potencjalnych konfliktów adresów IP w wypadku konfigurowania połączenia VPN pomiędzy sieciami o podobnych schematach adresowania. Typowy scenariusz dotyczy sytuacji, w której oba przedsiębiorstwa chcą utworzyć połączenia VPN, korzystając z tego samego zakresu prywatnych adresów IP. Na przykład 10.\*.\*. Sposób konfigurowania tego typu translacji VPN NAT zależy od tego, czy serwer lokalny jest inicjatorem, czy respondentem w połączeniu VPN. Kiedy serwer jest inicjatorem połączenia, można dokonać translacji adresów lokalnych na adresy zgodne z adresami drugiej strony w połączeniu VPN. Jeśli serwer jest respondentem w tym połączeniu, można dokonać translacji adresów drugiej strony w połączeniu VPN na adresy zgodne z lokalnym schematem adresowania. Ten rodzaj translacji należy skonfigurować wyłącznie dla połączeń dynamicznych.

#### **Translacja VPN NAT w celu ukrycia adresów lokalnych**

Ten rodzaj translacji VPN NAT jest używany głównie do ukrycia rzeczywistych adresów IP lokalnego systemu poprzez ich translację na adres, który będzie dostępny publicznie. Podczas konfigurowania translacji VPN NAT można sprawić, żeby każdy publiczny adres IP był przekształcany na jeden z puli ukrytych adresów. Pozwala to również rozkładać natężenie ruchu skierowanego pod jeden adres (publiczny) na wiele adresów (prywatnych). Translacja VPN NAT dla adresów lokalnych wymaga, aby serwer pełnił w połączeniach rolę respondenta.

Jeśli odpowiedzi na poniższe pytania są twierdzące, należy używać translacji VPN NAT do ukrywania adresów lokalnych:

1. Czy w sieci jest przynajmniej jeden serwer, do którego użytkownicy powinni mieć dostęp poprzez połączenie VPN?
2. Czy wymaga się elastyczności w zakresie rzeczywistych adresów IP lokalnych systemów?
3. Czy firma dysponuje przynajmniej jednym publicznym adresem IP?

W scenariuszu *“Scenariusz VPN: Wykorzystanie translacji adresów sieciowych na potrzeby sieci VPN” na stronie 19* przedstawiono przykład konfiguracji translacji VPN NAT w celu ukrycia lokalnego adresu serwera iSeries<sup>(TM)</sup>.

Instrukcje opisujące krok po kroku konfigurowanie translacji VPN NAT na serwerze iSeries znajdują się w pomocy elektronicznej dostępnej z interfejsu VPN w programie iSeries Navigator.

## **Zgodność translacji NAT i protokołów IPSec**

### **Problem: Konwencjonalna translacja NAT przerywa połączenia VPN**

Translacja adresów sieciowych (NAT) umożliwia ukrycie niezarejestrowanych adresów prywatnych za zbiorem zarejestrowanych adresów IP. Jest to przydatne przy zabezpieczaniu sieci wewnętrznej przed sieciami zewnętrznymi. Translacja NAT pomaga także uporać się z problemem wyczerpywania się dostępnych adresów IP, ponieważ pozwala odwzorować wiele adresów prywatnych na niewielki zbiór adresów zarejestrowanych.

Niestety, konwencjonalna translacja NAT nie współdziała z pakietami protokołów IPSec, ponieważ w pakiecie przechodzącym przez urządzenie NAT zmienia się adres źródłowy, co powoduje unieważnienie pakietu. W takiej sytuacji strona odbierająca w połączeniu VPN odrzuca pakiet i próba negocjowania połączenia VPN kończy się niepowodzeniem.

### Rozwiązanie: Hermetyzacja UDP

Ujmując rzecz w skrócie, hermetyzacja UDP polega na opakowaniu pakietu IPSec nowym, chociaż zduplikowanym, nagłówkiem IP/UDP. Podczas przejścia przez urządzenie NAT translacji zostaje poddany nowy nagłówek IP. Następnie, kiedy pakiet dociera do celu, strona odbierająca usuwa ten dodatkowy nagłówek i pozostawia oryginalny pakiet IPSec, który przedzie wszystkie pozostałe sprawdziany poprawności.

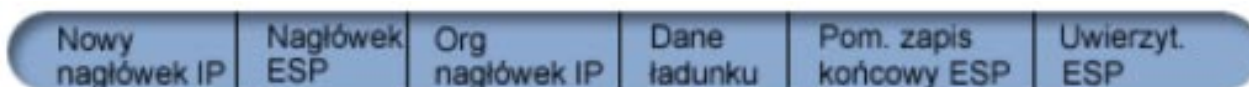
Hermetyzację UDP można stosować wyłącznie z protokołem IPSec ESP w trybie transportowym albo tunelowym. Ponadto w wersji V5R2 serwer iSeries<sup>(TM)</sup> może działać wyłącznie jako klient hermetyzacji UDP. Oznacza to, że może on tylko *inicjować* ruch z hermetyzacją UDP.

Poniższy rysunek przedstawia format pakietu protokołu ESP z hermetyzacją UDP w trybie tunelowym:

#### Oryginalny datagram IPv4:



#### Po zastosowaniu protokołu IPSec ESP w trybie tunelowym:

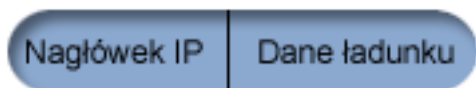


#### Po zastosowaniu hermetyzacji UDP:

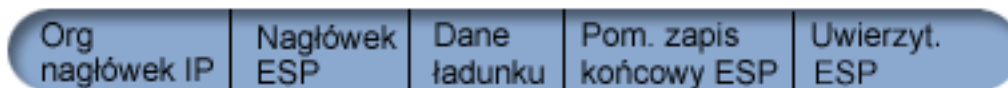


Poniższy rysunek przedstawia format pakietu ESP z hermetyzacją UDP w trybie transportowym:

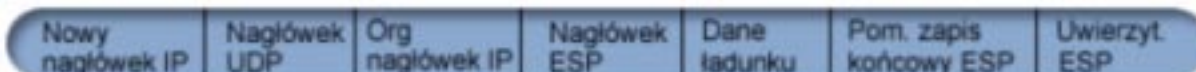
#### Oryginalny datagram IPv4:



#### Po zastosowaniu protokołu IPSec ESP w trybie transportowym:



#### Po zastosowaniu hermetyzacji UDP:



» Po zastosowaniu hermetyzacji pakietu, serwer iSeries wysyła pakiet do swojego partnera w połączeniu VPN poprzez port protokołu UDP o numerze 4500. Zazwyczaj obie strony połączenia VPN przeprowadziły już negocjacje IKE poprzez port UDP 500. Jednakże gdy podczas negocjacji klucza protokoły IKE wykryją translację NAT, następne pakiety IKE są wysyłane przez port źródłowy 4500 i port docelowy 4500. Oznacza to również, że dla portu 4500 nie mogą być włączone żadne reguły filtrowania. Strona odbierająca połączenie może rozpoznać, czy pakiet jest pakietem

IKE, czy też zahermetyzowanym pakietem UDP na podstawie pierwszych czterech bajtów danych właściwych UDP, które w pakiecie IKE mają wartość 0. Aby rozwiązanie to działało poprawnie, niezbędne jest, aby obie strony połączenia obsługiwały hermetyzację UDP. <<

## Protokół IP Compression (IPComp)

Protokół kompresji danych właściwych IP (IP Payload Compression - IPComp) pozwala zredukować wielkość datagramów IP przez poddanie ich kompresji. Prowadzi to do zwiększenia wydajności łącza komunikacyjnego pomiędzy dwoma stronami połączenia VPN. Jest to szczególnie użyteczne w wypadku komunikacji przez wolne lub przeciążone łącza. Protokół IPComp nie zapewnia żadnych mechanizmów ochronnych i w wypadku połączeń VPN musi być używany z protokołem AH lub ESP.

Formalna definicja protokołu IPComp została opublikowana przez grupę wykonawczą IETF (Internet Engineering Task Force) w dokumencie Request for Comments (RFC) 2393 zatytułowanym *IP Payload compression Protocol (IPComp)*.

Dokument ten jest dostępny w serwisie internetowym: <http://www.rfc-editor.org> .

## Sieci VPN i filtrowanie IP

Większość połączeń VPN wymaga do prawidłowej pracy reguł filtrowania. Reguły te zależą od typu konfigurowanego połączenia VPN, a także od rodzaju ruchu, który ma być kontrolowany. Zwykle każde połączenie będzie miało filtr strategii. Filtry strategii określają adresy, protokoły i porty, które mogą używać połączeń VPN. Dodatkowo połączenia obsługujące protokół Internet Key Exchange (IKE) mają zazwyczaj reguły zezwalające wprost na przetwarzanie negocjacji IKE.

Począwszy od systemu operacyjnego w wersji V5R1, połączenia VPN mogą generować te reguły automatycznie. Zawsze wtedy, gdy jest to możliwe, pozwól modułowi VPN wygenerować filtry strategii. Pozwoli to wyeliminować błędy oraz uniknąć konfigurowania reguł w osobnym kroku za pomocą Edytora reguł pakietów w programie iSeries<sup>(TM)</sup> Navigator.

Od tych zasad są jednak wyjątki. Dzięki lekturze poniższych sekcji, użytkownik pozna inne, mniej popularne koncepcje i techniki dotyczące połączeń VPN i filtrowania, które można zastosować w indywidualnych sytuacjach:

- **“Migracja filtrów strategii do bieżącej wersji systemu”**  
W wersjach V4R4 i V4R5 systemu operacyjnego konieczne było konfigurowanie reguł pakietów VPN w osobnym kroku. Nie były one generowane automatycznie w ramach konfigurowania połączeń VPN. W tej sekcji opisano szczegółowo zagadnienia dotyczące migracji filtrów strategii z wersji V4R4 i V4R5 do wersji obecnej.
- **“Połączenie VPN bez filtrów strategii” na stronie 30**  
Jeśli punkty końcowe połączenia VPN są pojedynczymi, konkretnymi adresami IP i chce się uruchomić połączenie bez konieczności pisania lub uaktywniania w systemie reguł filtrowania, można skonfigurować dynamiczny filtr strategii. W sekcji tej opisano, kiedy takie rozwiązanie można brać pod uwagę i jak je wdrożyć.
- **“Niejawne zezwolenie na ruch danych IKE” na stronie 31**  
Aby umożliwić negocjacje IKE dla połączenia VPN, należy pozwolić na przesyłanie przez port 500 datagramów UDP z tym typem danych IP. Jeśli jednak w systemie nie ma reguł filtrowania, które dopuszczałyby ruch danych IKE, wówczas system umożliwi taki ruch w sposób niejawni. Ta sekcja zawiera dodatkowe informacje o takich przypadkach w systemach iSeries.

## Migracja filtrów strategii do bieżącej wersji systemu

W wersjach V4R4 i V4R5 systemu operacyjnego konieczne było konfigurowanie reguł pakietów VPN w osobnym kroku za pomocą interfejsu Reguły pakietów w programie iSeries<sup>(TM)</sup> Navigator. Nie były one generowane automatycznie w ramach konfigurowania połączeń VPN. Począwszy od systemu operacyjnego w wersji V5R1, interfejs GUI połączeń VPN może generować te reguły automatycznie.

Aby w bieżącej wersji systemu korzystać z reguł filtrowania strategii (reguł, dla których parametr ACTION=IPSEC) utworzonych w wersjach V4R4 lub V4R5, należy wziąć pod uwagę kilka zagadnień. Dotyczy to również sytuacji, w której interfejs VPN *wygeneruje* reguły filtrowania strategii, ale potrzebne będą dodatkowe reguły umożliwiające przesyłanie połączeniem innego ruchu IP, na przykład danych programu Telnet. Aby uniknąć potencjalnych błędów konfiguracyjnych, należy postępować zgodnie z poniższymi zaleceniami.

**Objaśnienie:** Kiedy w tej sekcji następuje odwołanie do pliku reguł *klienta*, chodzi o wszelkie pliki reguł utworzone za pomocą edytora reguł pakietów w programie iSeries Navigator. W odróżnieniu od tych plików, plik reguł *VPNPOLICYFILTERS.I3P* jest plikiem wygenerowanym automatycznie w ramach konfigurowania połączeń VPN.

- Jeśli w systemie istnieją definicje połączeń VPN z wersji V4R4 lub V4R5 i nie planuje się konfigurowania innych połączeń w wersji bieżącej, można w zwykły sposób uaktywnić reguły filtrowania i uruchomić te połączenia.
- Jeśli w systemie istnieją definicje połączeń VPN z wersji V4R4 lub V4R5 i planuje się skonfigurowanie nowych połączeń VPN w bieżącej wersji, należy użyć **Kreatora migracji filtrów strategii**. Kreator ten usunie filtry strategii z utworzonych wcześniej plików reguł filtrowania i wstawi równoważne filtry strategii do pliku *VPNPOLICYFILTERS.I3P* wygenerowanego przez VPN. Aby uzyskać do niego dostęp, wykonaj następujące czynności:
  1. W programie iSeries Navigator rozwiń pozycję serwer —>**Sieć** —>**Strategie IP**.
  2. Prawym przyciskiem myszy kliknij pozycję **Sieć VPN** i wybierz opcję **Migrowanie filtrów strategii**.
  3. Po wykonaniu przycisku w kreatorze kliknij przycisk **Zakończ**.
  4. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
- Jeśli reguły filtrowania strategii zostały wygenerowane przez VPN, ale zachodzi potrzeba dodania innych reguł, należy je skonfigurować za pomocą Edytora reguł pakietów w programie iSeries Navigator. W przypadku, kiedy dowolne z dodatkowych reguł filtrowania powinny zostać użyte przed filtry VPN, należy poprzedzić nazwę zestawu takich reguł przedrostkiem **PREIPSEC**. Na przykład **PREIPSECMOJEREG**. Pomoże to systemowi określić kolejność przetwarzania reguł filtrowania. Nazwy zestawów pozostałych reguł innych niż VPN nie mogą mieć przedrostka **PREIPSEC**. Na przykład **INNEREG**.
- Zawsze należy umożliwić interfejsowi VPN wygenerowanie reguł filtrowania strategii. Jednak reguły filtrowania inne niż VPN muszą pozostać w pliku reguł klienta. Należy pamiętać, że jeśli jakaś reguła inna niż VPN musi zostać użyta przed filtry strategii z pliku reguł *VPNPOLICYFILTERS.I3P*, konieczne jest poprzedzenie nazwy zestawu takich reguł przedrostkiem **PREIPSEC**. Umożliwi to prawidłową współpracę reguł klienta i reguł VPN. Rozważmy przykład, w którym interfejs VPN wygenerował reguły filtrowania strategii (zestawy VPN), ale użytkownik utworzył dodatkowe reguły (zestawy Inne), aby umożliwić przesyłanie przez połączenie innego ruchu IP. Po załadowaniu reguł w systemie będą one przetwarzane w następującej kolejności:
  1. zestawy Inne, których nazwy zaczynają się od przedrostka **PREIPSEC**,
  2. zestawy VPN, których nazwy zaczynają się od przedrostka **PREIPSEC**,
  3. zestawy VPN z parametrem **ACTION=IPSEC** (filtry strategii),
  4. zestawy Inne z parametrem **ACTION=IPSEC** (filtry strategii),
  5. zestawy Inne z pozostałymi regułami,
  6. zestawy VPN z pozostałymi regułami.

Aby zobaczyć kolejność plików wejściowych w połączonym pliku wyjściowym, należy sprawdzić plik *EXPANDED.OUT*. Jest on zapisany w katalogu, w którym znajduje się plik reguł klienta.

- W programie iSeries Navigator można uaktywnić następujące reguły:
  - wyłącznie wygenerowane przez VPN reguły z pliku *VPNPOLICYFILTERS.I3P*,
  - wyłącznie reguły z pliku reguł klienta,
  - zarówno reguły wygenerowane przez VPN, jak i reguły z pliku reguł klienta.
- Reguły filtrowania należy uaktywnić dla wszystkich interfejsów, a nie dla poszczególnych interfejsów. Zagwarantuje to uaktywnienie filtrów strategii oraz zapewni ich prawidłową kolejność.
- Reguły filtrowania należy zawsze zweryfikować przed ich uaktywnieniem. Jeśli weryfikacja przebiegnie bez błędów, można sprawdzić w pliku *EXPANDED.OUT*, czy reguły są przetwarzane w odpowiedniej kolejności. Po wykonaniu tej czynności można uaktywnić reguły.

## Połączenie VPN bez filtrów strategii

Reguła filtrowania strategii określa adresy, protokoły i porty, które mogą korzystać z połączenia VPN i kieruje odpowiedni ruch poprzez połączenie. W niektórych przypadkach może zaistnieć potrzeba skonfigurowania połączenia, które nie wymaga reguły filtrowania strategii. Może się zdarzyć na przykład, że reguły pakietów inne niż VPN są już załadowane na interfejsie, z którego będzie korzystać połączenie VPN. Zamiast więc dezaktywować reguły na tym interfejsie można skonfigurować połączenie tak, że system będzie dynamicznie zarządzał wszystkimi filtry dla tego

połączenia. Filtr strategii dla połączenia tego typu nazywa się **dynamicznym filtrem strategii**. Aby można było korzystać z dynamicznego filtra strategii dla połączenia, muszą być spełnione następujące warunki:

- połączenia mogą być inicjowane tylko przez lokalny serwer,
- punkty końcowe danych w połączeniu muszą być pojedynczymi systemami; nie może to być podsieć ani zakres adresów,
- nie można załadować żadnej reguły filtrowania strategii dla połączenia.

Jeśli dane połączenie spełnia te kryteria, można je skonfigurować w taki sposób, aby nie wymagało ono filtra strategii. Po uruchomieniu połączenia dane pomiędzy punktami końcowymi będą przesyłane niezależnie od innych reguł pakietów załadowanych w systemie.

Instrukcje, opisujące krok po kroku konfigurowanie połączenia, które nie wymaga filtra strategii, znajdują się w pomocy elektronicznej dla interfejsu VPN.

## Niejawne zezwolenie na ruch danych IKE

W większości połączeń VPN wymaga się, aby przed przetwarzaniem danych przesyłanych protokołem IPSec odbyły się negocjacje IKE (Internet Key Exchange). Protokół IKE korzysta z ogólnie znanego portu 500, aby więc umożliwić jego prawidłowe działanie, należy pozwolić na przesyłanie przez port 500 datagramów UDP z tym typem danych IP. Jeśli jednak w systemie nie ma reguł filtrowania, które dopuszczająby ruch danych IKE, wówczas zezwolenie na taki ruch ma charakter niejawny. Reguły napisane specjalnie dla wykorzystywanego przez protokół UDP portu 500 są obsługiwane zgodnie z aktywnymi regułami filtrowania.

---

## Planowanie sieci VPN

Planowanie to zasadniczy element całego rozwiązania VPN. Aby zapewnić prawidłowe działanie połączeń, trzeba podjąć wiele złożonych decyzji. Wymienione niżej zasoby pozwolą zebrać wszystkie informacje niezbędne do tego, by implementacja sieci VPN zakończyła się powodzeniem:

- “Wymagania konfiguracyjne VPN”  
Na początku sprawdź, czy zostały spełnione minimalne wymagania dotyczące utworzenia sieci VPN.
- “Określenie typu tworzonej sieci VPN” na stronie 32  
Jednym z pierwszych etapów planowania jest określenie sposobu wykorzystania połączeń VPN. W tej sekcji opisano różne typy połączeń, jakie można skonfigurować.
- **Korzystanie z doradcy podczas planowania sieci VPN**  
Doradca w zakresie planowania zadaje użytkownikowi pytania dotyczące danej sieci i na podstawie udzielonych odpowiedzi przedstawia sugestie związane z tworzeniem sieci VPN.  
**Uwaga:** Z doradcy w zakresie planowania VPN można korzystać tylko w wypadku połączeń obsługujących protokół IKE (Internet Key Exchange). Dla połączeń typu ręcznego należy skorzystać z arkusza planowania.
- “Arkusze planowania VPN” na stronie 33  
Wydrukowane i wypełnione arkusze planowania są źródłem szczegółowych informacji dotyczących planów wykorzystania sieci VPN.

Po opracowaniu planu sieci VPN można przystąpić do jej “Konfigurowanie połączeń VPN” na stronie 36.

## Wymagania konfiguracyjne VPN

Aby połączenia VPN mogły prawidłowo funkcjonować, serwer iSeries<sup>(TM)</sup> i klienci PC muszą spełniać następujące wymagania:

### Wymagania serwera iSeries V5R2



- System operacyjny OS/400<sup>(R)</sup> wersja 5 wydanie 2 (5722-SS1) lub nowszy,
- Menedżer certyfikatów cyfrowych (5722-SS1 opcja 34),
- Cryptographic Access Provider (5722-AC2 lub AC3),
- iSeries Access for Windows<sup>(R)</sup>(5722-XE1) i iSeries Navigator,
  - komponent Sieć programu iSeries Navigator,
- wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC \*SEC) ustawiona na 1,
- skonfigurowany protokół TCP/IP, w tym interfejsy IP, trasy, nazwa lokalnego hosta i nazwa lokalnej domeny.

#### **Wymagania klienta**

- stacja robocza z 32-bitowym systemem operacyjnym Windows<sup>(R)</sup>, prawidłowo podłączona do serwera iSeries i skonfigurowana do obsługi TCP/IP,
- procesor o częstotliwości 233 MHz,
- 32 MB pamięci RAM dla klientów Windows 95/98,
- 64 MB pamięci RAM dla klientów Windows NT<sup>(R)</sup> i 2000
- programy iSeries Access for Windows i iSeries Navigator zainstalowane na klienckim komputerze PC,
- oprogramowanie obsługujące protokół IPSec (IP Security),
- oprogramowanie obsługujące protokół L2TP, jeśli zdalni użytkownicy będą używali tego protokołu do nawiązywania połączeń z lokalnym systemem.

## **Określenie typu tworzonej sieci VPN**

Jednym z pierwszych etapów planowania jest określenie sposobu wykorzystania połączeń VPN. Niezbędna jest do tego znajomość ról, jakie w połączeniu pełnić będą lokalny i zdalny serwer kluczy. Zależy to na przykład od tego, czy punkty końcowe *połączenia* są różne od punktów końcowych *danych*. Mogą one być takie same lub różnić się tylko po jednej stronie połączenia. Punkty końcowe połączenia uwierzytelniają i szyfrują (lub deszyfrują) dane przesyłane połączeniem oraz opcjonalnie zarządzają kluczami w ramach protokołu IKE (Internet Key Exchange). Natomiast punkty końcowe danych wyznaczają połączenie pomiędzy dwoma systemami dla danych IP przesyłanych połączeniem VPN; na przykład cały ruch TCP/IP pomiędzy adresami 123.4.5.6 i 123.7.8.9. W większości przypadków, kiedy punkty końcowe połączenia i danych różnią się, serwer VPN pełni rolę bramy. Kiedy punkty te pokrywają się, serwer VPN jest hostem.

Spośród różnych typów implementacji VPN, które odpowiadają potrzebom większości przedsiębiorstw, wymienić należy:

#### **Połączenie między bramami**

Punkty końcowe połączenia w obydwu systemach są różne od punktów końcowych danych. Dane przesyłane pomiędzy bramami są zabezpieczone za pomocą protokołu IPSec. Protokół ten nie chroni jednak danych poza bramami, w sieciach wewnętrznych po obydwu stronach połączenia. Konfiguracja taka jest często stosowana dla połączeń pomiędzy oddziałami przedsiębiorstwa, ponieważ sieci wewnętrzne oddziałów są często uważane za sieci zaufane.

#### **Połączenie między bramą i hostem**

Protokół IPSec chroni dane przesyłane pomiędzy bramą a hostem w zdalnej sieci. Połączenie VPN nie zabezpiecza danych w sieci lokalnej, ponieważ jest ona uznawana za zaufaną.

#### **Połączenie między hostem i bramą**

Połączenie VPN chroni dane przesyłane pomiędzy hostem w sieci lokalnej a bramą. Dane w sieci zdalnej nie są chronione.

#### **Połączenie między hostami**

Zarówno w systemie lokalnym, jak i zdalnym punkty końcowe połączenia pokrywają się z punktami końcowymi danych. Połączenie VPN chroni dane przesyłane pomiędzy hostem w sieci lokalnej a hostem w sieci zdalnej. W połączeniu VPN tego rodzaju dane są chronione na całej trasie za pomocą protokołu IPSec.

## Arkusze planowania VPN

Arkusze planowania służą do zbierania szczegółowych informacji dotyczących planów wykorzystania sieci VPN. Informacje te są potrzebne do odpowiedniego zaplanowania strategii implementacji VPN. Mogą one także posłużyć do konfigurowania połączeń VPN. Należy wybrać arkusz odpowiedni do rodzaju połączenia, które ma zostać utworzone.

- “Arkusz planowania dla połączeń dynamicznych”  
Arkusz ten należy wypełnić przed przystąpieniem do skonfigurowania połączenia dynamicznego.
- “Arkusz planowania dla połączeń ręcznych” na stronie 34  
Arkusz ten należy wypełnić przed przystąpieniem do skonfigurowania połączenia ręcznego.
- **Doradca w zakresie planowania VPN**  
Można także skorzystać z doradcy, który oferuje interaktywną pomoc w zakresie planowania i konfigurowania. Doradca w zakresie planowania zadaje użytkownikowi pytania dotyczące danej sieci i na podstawie udzielonych odpowiedzi przedstawia sugestie związane z tworzeniem sieci VPN.  
**Uwaga:** Z doradcy w zakresie planowania VPN można korzystać tylko w wypadku połączeń dynamicznych. Dla połączeń typu ręcznego należy skorzystać z arkusza planowania.

W sytuacji, kiedy tworzonych będzie wiele połączeń o podobnych właściwościach, można ustawić domyślne ustawienia połączeń VPN. Skonfigurowane wartości domyślne są używane do wstępnego wypełnienia arkuszy właściwości połączeń VPN. Oznacza to, że nie ma potrzeby wielokrotnego konfigurowania tych samych właściwości. Aby ustawić domyślne parametry wartości ustawień VPN, należy wybrać opcję **Edycja** z głównego menu VPN, a następnie wybrać opcję **Wartości domyślne**.

### Arkusz planowania dla połączeń dynamicznych

Przed utworzeniem dynamicznych połączeń VPN należy wypełnić poniższy arkusz. Arkusz został skonstruowany przy założeniu, że użytkownik będzie korzystał z Kreatora nowego połączenia. Kreator ten umożliwi skonfigurowanie VPN na podstawie podstawowych wymagań w zakresie ochrony. W niektórych przypadkach konieczne może być wprowadzenie drobnych korekt we właściwościach połączenia skonfigurowanych przez kreatora. Można na przykład włączyć kronikowanie lub zdecydować o uruchamianiu serwera VPN zawsze podczas uruchamiania protokołu TCP/IP. Należy wtedy kliknąć prawym przyciskiem myszy grupę z kluczem dynamicznym lub połączenie utworzone przez kreatora i wybrać opcję **Właściwości**.

Przed przystąpieniem do konfigurowania połączeń VPN odpowiedz na wszystkie pytania w poniższym formularzu.

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy system operacyjny to OS/400 <sup>(R)</sup> wersja V5R2 (5722-SS1) lub nowsza?	
Czy zainstalowano opcję Digital Certificate Manager (5722-SS1 opcja 34)?	
Czy zainstalowano produkt Cryptographic Access Provider (5722-AC2 lub AC3)?	
Czy zainstalowano produkt iSeries <sup>(TM)</sup> Access(5722-XE1)?	
Czy zainstalowano program iSeries Navigator?	
Czy zainstalowano komponent Sieć programu iSeries Navigator?	
Czy zainstalowano produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	
Czy na serwerze iSeries skonfigurowano protokół TCP/IP (w tym interfejsy IP, trasy, nazwę lokalnego hosta i nazwę lokalnej domeny)?	
Czy pomiędzy obydwoma punktami końcowymi nawiązano normalne połączenie TCP/IP?	
Czy zastosowano najnowsze poprawki PTF?	
Czy w wypadku, kiedy tunel VPN przechodzi przez firewalle lub routery korzystające z filtracji pakietów IP, reguły filtrowania firewalla lub routera obsługują protokoły AH i ESP?	
Czy konfiguracja firewalli lub routerów umożliwia stosowanie protokołów IKE (port UDP 500), AH i ESP?	
Czy konfiguracja firewalli umożliwia przekazywanie IP?	

Informacje potrzebne do skonfigurowania dynamicznego połączenia VPN	Odpowiedzi
Jakiego typu połączenie jest tworzone? <ul style="list-style-type: none"> <li>• Między bramami</li> <li>• Między hostem i bramą</li> <li>• Między bramą i hostem</li> <li>• Między hostami</li> </ul>	
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony kluczy? <ul style="list-style-type: none"> <li>• Najwyższa ochrona, najniższa wydajność</li> <li>• Zrównoważona ochrona i wydajność</li> <li>• Najniższa ochrona i najwyższa wydajność</li> </ul>	
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	
Jaki jest identyfikator lokalnego serwera kluczy?	
Jaki jest identyfikator lokalnego punktu końcowego danych?	
Jaki jest identyfikator zdalnego serwera kluczy?	
Jaki jest identyfikator zdalnego punktu końcowego danych?	
Jakiego typu ochrony i wydajności systemu wymaga się do ochrony danych? <ul style="list-style-type: none"> <li>• Najwyższa ochrona, najniższa wydajność</li> <li>• Zrównoważona ochrona i wydajność</li> <li>• Najniższa ochrona i najwyższa wydajność</li> </ul>	

## Arkusz planowania dla połączeń ręcznych

Po wypełnieniu tego arkusza będzie można z niego skorzystać podczas tworzenia połączeń wirtualnych sieci prywatnych (VPN), które nie używają protokołu IKE do zarządzania kluczami.

Przed przystąpieniem do konfigurowania połączeń VPN należy odpowiedzieć na wszystkie pytania w poniższym formularzu:

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy system operacyjny to OS/400 <sup>(R)</sup> wersja V5R2 (5722-SS1) lub nowsza?	
Czy zainstalowano opcję Digital Certificate Manager (5722-SS1 opcja 34)?	
Czy zainstalowano produkt Cryptographic Access Provider (5722-AC2 lub AC3)?	
Czy zainstalowano produkt iSeries <sup>(TM)</sup> Access(5722-XE1)?	
Czy zainstalowano program iSeries Navigator?	
Czy zainstalowano komponent Sieć programu iSeries Navigator?	
Czy zainstalowano produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	
Czy na serwerze iSeries skonfigurowano protokół TCP/IP (w tym interfejsy IP, trasy, nazwę lokalnego hosta i nazwę lokalnej domeny)?	
Czy pomiędzy obydwojema punktami końcowymi nawiązano normalne połączenie TCP/IP?	
Czy zastosowano najnowsze poprawki PTF?	
Czy w wypadku, kiedy tunel VPN przechodzi przez firewalle lub routery korzystające z filtracji pakietów IP, reguły filtrowania firewalle lub routera obsługują protokoły AH i ESP?	
Czy konfiguracja firewalle lub routerów umożliwia stosowanie protokołów AH i ESP?	



Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy konfiguracja firewalli umożliwia przekazywanie IP?	

Informacje potrzebne do skonfigurowania ręcznych połączeń VPN	Odpowiedzi
<p>Jakiego typu połączenie jest tworzone?</p> <ul style="list-style-type: none"> <li>• Między hostami</li> <li>• Między hostem i bramą</li> <li>• Między bramą i hostem</li> <li>• Między bramami</li> </ul>	
Jaka nazwa zostanie nadana połączeniu?	
Jaki jest identyfikator lokalnego punktu końcowego połączenia?	
Jaki jest identyfikator zdalnego punktu końcowego połączenia?	
Jaki jest identyfikator lokalnego punktu końcowego danych?	
Jaki jest identyfikator zdalnego punktu końcowego danych?	
Jaki rodzaj ruchu jest dozwolony dla tego połączenia (port lokalny, port zdalny i protokół)?	
Czy dla tego połączenia wymagana jest translacja adresów sieciowych? Więcej informacji na ten temat zawiera sekcja “Translacja adresów sieciowych dla sieci VPN” na stronie 26.	
Czy będzie wykorzystywany tryb tunelowy, czy transportowy?	
Z jakiego protokołu IPSec będzie korzystało połączenie (AH, ESP lub AH z ESP)? Więcej informacji na ten temat zawiera sekcja “Protokoły IP Security (IPSec)” na stronie 21.	
Z jakiego algorytmu uwierzytelniania będzie korzystało połączenie (HMAC-MD5 lub HMAC-SHA)?	
Z jakiego algorytmu szyfrowania będzie korzystało połączenie (DES-CBC lub 3DES-CBC)?	
<b>Uwaga:</b> Algorytm szyfrowania należy określić tylko wtedy, gdy jako protokół IPSec wybrano ESP.	
<p>Jaki jest klucz przychodzący protokołu AH? W wypadku stosowania algorytmu MD5 kluczem jest 16-bajtowy łańcuch szesnastkowy. Jeśli używa się algorytmu SHA, kluczem jest 20-bajtowy łańcuch szesnastkowy.</p> <p>Klucz przychodzący musi dokładnie odpowiadać kluczowi wychodzącemu zdalnego serwera.</p>	
<p>Jaki jest klucz wychodzący protokołu AH? W wypadku stosowania algorytmu MD5 kluczem jest 16-bajtowy łańcuch szesnastkowy. Jeśli używany jest algorytm SHA, kluczem jest 20-bajtowy łańcuch szesnastkowy.</p> <p>Klucz wychodzący musi dokładnie odpowiadać kluczowi przychodzącemu zdalnego serwera.</p>	
<p>Jaki jest klucz przychodzący protokołu ESP? Jeśli używany jest algorytm szyfrowania DES, kluczem jest 8-bajtowy łańcuch szesnastkowy. W wypadku szyfrowania algorytmem 3DES kluczem jest 24-bajtowy łańcuch szesnastkowy.</p> <p>Klucz przychodzący musi dokładnie odpowiadać kluczowi wychodzącemu zdalnego serwera.</p>	
<p>Jaki jest klucz wychodzący protokołu ESP? Jeśli używany jest algorytm szyfrowania DES, kluczem jest 8-bajtowy łańcuch szesnastkowy. W wypadku szyfrowania algorytmem 3DES kluczem jest 24-bajtowy łańcuch szesnastkowy.</p> <p>Klucz wychodzący musi dokładnie odpowiadać kluczowi przychodzącemu zdalnego serwera.</p>	
<p>Jaki jest przychodzący indeks strategii ochrony (Security Policy Index -SPI)? Przychodzący indeks SPI jest 4-bajtowym łańcuchem szesnastkowym, w którym pierwszy bajt ma wartość 00.</p> <p>Przychodzący indeks SPI musi dokładnie odpowiadać wychodzącemu indeksowi SPI zdalnego serwera.</p>	

Informacje potrzebne do skonfigurowania ręcznych połączeń VPN	Odpowiedzi
Jaki jest wychodzący indeks SPI? Wychodzący indeks SPI jest 4-bajtowym łańcuchem szesnastkowym.	
Wychodzący indeks SPI musi dokładnie odpowiadać przychodzącemu indeksowi SPI zdalnego serwera.	

## Konfigurowanie połączeń VPN

W interfejsie VPN dostępnych jest kilka różnych sposobów konfigurowania połączeń VPN. Przedstawione poniżej informacje pomogą zdecydować, jaki typ połączenia skonfigurować i jak to zrobić.

### Wybór typu konfigurowanego połączenia

Połączenie **dynamiczne** to takie, w którym, gdy jest ono aktywne, klucze chroniące to połączenie są generowane i negocjowane dynamicznie, przy użyciu protokołu Internet Key Exchange (IKE). Połączenia dynamiczne zapewniają dodatkowy poziom ochrony przesyłanych danych dzięki automatycznej zmianie kluczy w regularnych odstępach czasu. W rezultacie zmniejsza się prawdopodobieństwo przechwycenia klucza przez osobę niepowołaną, a także skraca czas, w którym mogłaby ona złamać klucz i użyć go do zmiany lub przechwycenia danych zabezpieczonych tym kluczem.

Połączenie **ręczne (Str. 37)** natomiast nie obsługuje negocjacji IKE ani tym samym automatycznego zarządzania kluczami. Co więcej, konieczne jest skonfigurowanie po obu stronach połączenia kilku atrybutów w taki sposób, aby dokładnie sobie odpowiadały. W połączeniach ręcznych używane są klucze statyczne, które nie są odświeżane ani zmieniane w czasie, gdy połączenie jest aktywne. Aby zmienić klucz powiązany z połączeniem ręcznym, należy je zakończyć. Jeśli w danej sytuacji powyższe czynniki zagrażają bezpieczeństwu, zamiast połączenia ręcznego można skonfigurować połączenie dynamiczne.

### Konfigurowanie dynamicznego połączenia VPN

Połączenie VPN to w rzeczywistości grupa obiektów konfiguracyjnych definiujących charakterystyki połączenia. Dynamiczne połączenie VPN wymaga, aby każdy z tych obiektów działał prawidłowo. Poniżej zamieszczono odsyłacze do szczegółowych informacji dotyczących sposobu konfigurowania każdego z obiektów konfiguracyjnych połączenia VPN:

#### Wskazówka:

“Konfigurowanie połączeń za pomocą Kreatora nowego połączenia” na stronie 38

Ogólnie biorąc do tworzenia wszystkich połączeń dynamicznych można użyć Kreatora połączeń. Kreator automatycznie tworzy wszystkie obiekty konfiguracyjne wymagane przez połączenie VPN do prawidłowego działania, w tym również reguły pakietów. Jeśli w kreatorze zostanie wybrane uaktywnienie reguł pakietów VPN, można pominąć przedstawiony poniżej punkt 6. *Uruchamianie połączenia*. W przeciwnym razie po zakończeniu konfigurowania połączenia VPN za pomocą kreatora konieczne jest uaktywnienie reguł pakietów i uruchomienie połączenia.

W razie podjęcia decyzji o samodzielnym skonfigurowaniu dynamicznych połączeń VPN należy wykonać poniższe czynności:

1. “Konfigurowanie strategii ochrony VPN” na stronie 38  
Dla wszystkich połączeń dynamicznych należy zdefiniować strategię ochrony. Strategia protokołu Internet Key Exchange i strategia danych określają sposób ochrony przez protokół IKE fazy 1. i 2. negocjacji.
2. “Konfigurowanie chronionego połączenia VPN” na stronie 39  
Po zdefiniowaniu strategii ochrony dla połączenia należy skonfigurować połączenie chronione. W przypadku połączeń dynamicznych obiekt połączenia chronionego zawiera grupę z kluczem dynamicznym i połączenie z kluczem dynamicznym. **Grupa z kluczem dynamicznym** określa właściwości wspólne dla kilku połączeń VPN, natomiast **połączenie z kluczem dynamicznym** określa charakterystyki indywidualnych połączeń danych pomiędzy parami punktów końcowych. Połączenie z kluczem dynamicznym istnieje w ramach grupy z kluczem dynamicznym.

**Uwaga:** Jeśli w interfejsie VPN na stronie **Grupa z kluczem dynamicznym - połączenia** wybrano opcję **Reguła filtrowania strategii zostanie zdefiniowana w regułach pakietów**, wystarczy tylko wykonać czynności opisane w dwóch następnych punktach: *Konfigurowanie reguł pakietów* i *Definiowanie interfejsu dla reguł*. W przeciwnym razie reguły te zostaną utworzone w ramach konfigurowania połączeń VPN i będą zastosowane do wskazanych interfejsów.

Zaleca się, aby zawsze umożliwić interfejsowi VPN wygenerowanie reguł filtrowania strategii. W tym celu należy wybrać opcję **Generuj poniższy filtr strategii dla tej grupy** na stronie **Grupa z kluczem dynamicznym - połączenia**.

3. “Konfigurowanie reguł pakietów VPN” na stronie 40

Po skonfigurowaniu połączeń VPN należy utworzyć i zastosować reguły filtrowania, które umożliwią przesyłanie danych przez połączenie. Reguły VPN typu **PREIPSEC** zezwalają na wymianę danych IKE przez określone interfejsy, a tym samym umożliwiają protokołowi IKE negocjowanie połączeń. Reguły **filtrowania strategii** definiują adresy, protokoły i porty, które mogą korzystać z powiązanej grupy z kluczem dynamicznym.

Jeśli wykonujesz migrację z wersji V4R4 lub V4R5 i zamierzasz wykorzystywać istniejące połączenia VPN i filtry strategii, zapoznaj się z sekcją “Migracja filtrów strategii do bieżącej wersji systemu” na stronie 29, aby zapewnić prawidłową współpracę starych i nowych filtrów strategii.

4. “Definiowanie interfejsu dla reguł filtrowania VPN” na stronie 43

Po skonfigurowaniu reguł pakietów i wszelkich innych reguł potrzebnych przy połączeniu VPN należy zdefiniować interfejs, dla którego zostaną one zastosowane.

5. “Uaktywnianie reguł pakietów VPN” na stronie 44

Po zdefiniowaniu interfejsu dla reguł pakietów należy je uaktywnić przed uruchomieniem połączenia.

6. “Uruchamianie połączenia VPN” na stronie 44

Wykonanie opisanych w tej sekcji zadań pozwoli uruchomić połączenie.

### Konfigurowanie ręcznego połączenia VPN

Zgodnie z nazwą połączenie ręczne wymaga samodzielnego skonfigurowania wszystkich właściwości VPN, w tym także kluczy przychodzących i wychodzących. Poniżej zamieszczono odsyłacze do szczegółowych informacji dotyczących konfigurowania połączenia ręcznego:

1. “Konfigurowanie połączeń ręcznych” na stronie 40

Połączenia ręczne definiują właściwości połączenia obejmujące protokoły ochrony oraz punkty końcowe danych.

**Uwaga:** Jeśli w interfejsie VPN na stronie **Połączenie ręczne - połączenie** wybrano opcję **Reguła filtrowania strategii zostanie zdefiniowana w regułach pakietów**, wystarczy tylko wykonać czynności opisane w dwóch następnych punktach: *Konfigurowanie reguły filtrowania strategii* i *Definiowanie interfejsu dla reguł*. W przeciwnym razie reguły te zostaną utworzone w ramach konfigurowania połączeń VPN.

Zaleca się, aby zawsze umożliwić interfejsowi VPN wygenerowanie reguł filtrowania strategii. W tym celu należy wybrać opcję **Generuj filtr strategii zgodny z punktami końcowymi danych** na stronie **Połączenie ręczne - połączenia**.

2. “Konfigurowanie reguły filtrowania strategii” na stronie 42

Po skonfigurowaniu atrybutów połączenia ręcznego należy utworzyć i zastosować regułę filtrowania strategii, która umożliwi przesyłanie danych przez połączenie. Reguła **filtrowania strategii** definiuje adresy, protokoły i porty, które mogą korzystać z powiązanego połączenia.

3. “Definiowanie interfejsu dla reguł filtrowania VPN” na stronie 43

Po skonfigurowaniu reguł pakietów i wszelkich innych reguł potrzebnych przy połączeniu VPN należy zdefiniować interfejs, dla którego zostaną one zastosowane.

4. “Uaktywnianie reguł pakietów VPN” na stronie 44

Po zdefiniowaniu interfejsu dla reguł pakietów należy je uaktywnić przed uruchomieniem połączenia.

5. “Uruchamianie połączenia VPN” na stronie 44

Wykonanie opisanych w tej sekcji zadań pozwoli uruchomić połączenie inicjowane lokalnie.

## Konfigurowanie połączeń za pomocą Kreatora nowego połączenia

Kreator nowego połączenia umożliwia utworzenie wirtualnej sieci prywatnej (VPN) łączącej dowolne hosty i bramy. Sieć ta może obejmować połączenia między hostami, między bramą i hostem, między hostem i bramą oraz między bramami.

Kreator automatycznie tworzy wszystkie obiekty konfiguracyjne wymagane przez połączenie VPN do prawidłowego działania, w tym również reguły pakietów. Jeśli jednak zachodzi potrzeba dodania jakiejś funkcji do konfiguracji VPN, na przykład kronikowania lub translacji adresów sieciowych dla połączeń VPN (VPN NAT), można dokonać zmian w arkuszach właściwości odpowiedniej grupy z kluczem dynamicznym lub połączenia. W tym celu należy najpierw zakończyć połączenie, jeśli jest ono aktywne. Następnie należy kliknąć prawym przyciskiem myszy grupę z kluczem dynamicznym lub połączenie i wybrać opcję **Właściwości**.

Przed rozpoczęciem należy odpowiedzieć na pytania Doradcy w zakresie planowania VPN. Doradca pomoże zebrać ważne informacje, które będą potrzebne do utworzenia połączenia VPN.

Aby utworzyć połączenie VPN za pomocą Kreatora połączeń, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**.
3. Postępuj zgodnie z instrukcjami kreatora, aby utworzyć podstawowe połączenie VPN. Jeśli będzie potrzebna pomoc, kliknij przycisk **Pomoc**.

## Konfigurowanie strategii ochrony VPN

Po zaplanowaniu sposobu korzystania z połączeń VPN należy zdefiniować strategię ochrony VPN. Zadanie to obejmuje przede wszystkim:

- “Konfigurowanie strategii protokołu Internet Key Exchange (IKE)”  
Strategia protokołu IKE określa poziom ochrony danych, za pomocą uwierzytelniania i szyfrowania, jaki będzie używany podczas fazy 1. negocjacji IKE. Podczas fazy 1. negocjacji IKE określone są klucze, które zabezpieczają wiadomości przesyłane następnie w fazie 2. negocjacji. W przypadku konfigurowania połączenia ręcznego nie ma potrzeby definiowania strategii protokołu IKE. Ponadto, jeśli połączenie VPN jest tworzone za pomocą Kreatora nowego połączenia, kreator może również utworzyć strategię protokołu IKE.
- “Konfigurowanie strategii danych” na stronie 39  
Strategia danych określa za pomocą uwierzytelniania i szyfrowania poziom ochrony, jaki zostanie użyty podczas przesyłania danych połączeniem VPN. Komunikujące się ze sobą systemy uzgadniają te atrybuty podczas fazy 2. negocjacji protokołu IKE. W przypadku konfigurowania połączenia ręcznego nie ma potrzeby definiowania strategii danych. Ponadto jeśli połączenie VPN jest tworzone za pomocą Kreatora nowego połączenia, kreator może również utworzyć strategię danych.

Po skonfigurowaniu strategii ochrony VPN należy przystąpić do konfigurowania “Konfigurowanie chronionego połączenia VPN” na stronie 39.

## Konfigurowanie strategii protokołu Internet Key Exchange (IKE)

Strategia protokołu IKE określa, za pomocą uwierzytelniania i szyfrowania, poziom ochrony stosowany przez protokół “Zarządzanie kluczami” na stronie 24 podczas fazy 2. negocjacji. Podczas fazy 1. negocjacji IKE określone są klucze, które zabezpieczają wiadomości przesyłane następnie w fazie 2. negocjacji. Do uwierzytelnienia fazy 1. negocjacji w połączeniu VPN używany jest albo podpis RSA, albo wstępne klucze współużytkowane. Planując wykorzystanie certyfikatów cyfrowych do uwierzytelniania serwerów kluczy, należy najpierw skonfigurować te certyfikaty w produkcie Menedżer certyfikatów cyfrowych (5722-SS1 opcja 34). Strategia IKE określa także, który zdalny serwer kluczy będzie z nich korzystał.

Aby zdefiniować nową lub zmienić istniejącą strategię IKE, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Strategia ochrony IP**.

2. Aby utworzyć nową strategię, kliknij prawym przyciskiem myszy pozycję **Strategia protokołu IKE** i wybierz opcję **Nowa strategia protokołu IKE**. Aby zmienić istniejącą strategię, kliknij pozycję **Strategia protokołu IKE** po lewej stronie okna, a następnie kliknij prawym przyciskiem myszy strategię, którą chcesz zmienić, i wybierz opcję **Właściwości**.
3. Wypełnij wszystkie arkusze właściwości. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Kliknij **OK**, aby zapisać wprowadzone zmiany.

» **Uwaga:** Zaleca się używanie głównego trybu uzgadniania zawsze wtedy, gdy do uwierzytelniania używany jest wstępny klucz współużytkowany. Zapewnia on bardziej bezpieczną wymianę. Jeśli konieczne jest użycie wstępnych kluczy współużytkowanych i agresywnego trybu uzgadniania, należy wybrać trudne hasła, których nie można złamać podczas ataku ze słownikiem. Zaleca się również okresowe zmiany haseł. Więcej informacji na ten temat zawiera pomoc elektroniczna programu iSeries Navigator. <<

## Konfigurowanie strategii danych

Strategia danych określa za pomocą uwierzytelniania i szyfrowania poziom ochrony, jaki zostanie użyty podczas przesyłania danych połączeniem VPN. Komunikujące się ze sobą systemy uzgadniają te atrybuty podczas fazy 2. negocjacji “Zarządzanie kluczami” na stronie 24.

Aby zdefiniować nową lub zmienić istniejącą strategię danych, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Strategia ochrony IP**.
2. Aby utworzyć nową strategię danych kliknij prawym przyciskiem myszy pozycję **Strategia danych** i wybierz opcję **Nowa strategia danych**. Aby zmienić istniejącą strategię, kliknij pozycję **Strategia danych** (po lewej stronie okna), a następnie kliknij prawym przyciskiem myszy strategię, którą chcesz zmienić, i wybierz opcję **Właściwości**.
3. Wypełnij wszystkie arkusze właściwości. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Kliknij **OK**, aby zapisać wprowadzone zmiany.

## Konfigurowanie chronionego połączenia VPN

Po zdefiniowaniu strategii ochrony dla połączenia należy skonfigurować połączenie chronione. W przypadku połączeń dynamicznych obiekt połączenia chronionego zawiera grupę z kluczem dynamicznym i połączenie z kluczem dynamicznym.

**Grupa z kluczem dynamicznym** określa cechy wspólne dla kilku połączeń VPN. Skonfigurowanie grupy z kluczem dynamicznym umożliwia wykorzystanie tych samych strategii dla wszystkich połączeń o różnych punktach końcowych danych należących do tej grupy. Ponadto grupy z kluczem dynamicznym umożliwiają pomyślne prowadzenie negocjacji ze zdalnymi inicjatorami także wtedy, gdy punkty końcowe danych proponowane przez system zdalny nie były wcześniej znane. Jest to możliwe dzięki powiązaniu informacji o strategii dla grupy z kluczem dynamicznym z regułą filtrowania strategii o czynności typu IPSEC. Jeśli punkty końcowe danych proponowane przez zdalny inicjator należą do zakresu określonego w regule filtrowania typu IPSEC, będą one podlegać strategii zdefiniowanej dla grupy z kluczem dynamicznym.

**Połączenie z kluczem dynamicznym** określa właściwości indywidualnych połączeń danych pomiędzy parami punktów końcowych. Połączenie z kluczem dynamicznym istnieje w ramach grupy z kluczem dynamicznym. Po skonfigurowaniu grupy z kluczem dynamicznym opisującej strategię, których używają połączenia z tej grupy, należy zdefiniować obiekty dla indywidualnych połączeń z kluczem dynamicznym, które będą inicjowane lokalnie.

Aby skonfigurować obiekt połączenia chronionego, wykonaj następujące czynności:

### Część 1: Konfigurowanie grupy z kluczem dynamicznym:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**.



2. Prawym przyciskiem myszy kliknij pozycję **Według grupy** i wybierz opcję **Nowa grupa połączeń z kluczem dynamicznym**.
3. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Kliknij **OK**, aby zapisać wprowadzone zmiany.

#### **Część 2: Konfigurowanie połączenia z kluczem dynamicznym:**

1. W programie iSeries Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione** → **Według grupy**.
2. W lewej części okna programu iSeries Navigator kliknij prawym przyciskiem myszy utworzoną w części pierwszej grupę z kluczem dynamicznym i wybierz opcję **Nowe połączenie z kluczem dynamicznym**.
3. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Kliknij **OK**, aby zapisać wprowadzone zmiany.

Po wykonaniu tych czynności należy “Uaktywnianie reguł pakietów VPN” na stronie 44 reguły pakietów wymagane przez połączenie do prawidłowego działania.

**Uwaga:** W większości przypadków należy umożliwić interfejsowi VPN automatyczne wygenerowanie reguł pakietów, wybierając na stronie **Grupa z kluczem dynamicznym - Połączenia** opcję **Generuj poniższy filtr strategii dla tej grupy**. Jeśli jednak wybrana zostanie opcja **Reguła filtrowania strategii zostanie zdefiniowana w regule pakietów**, trzeba będzie następnie “Konfigurowanie reguł pakietów VPN” przy użyciu Edytora reguł pakietów.

## **Konfigurowanie połączeń ręcznych**

Zgodnie z nazwą połączenie ręczne wymaga samodzielnego skonfigurowania wszystkich właściwości VPN. Co więcej, konieczne jest skonfigurowanie po obu stronach połączenia kilku elementów w taki sposób, aby *dokładnie* sobie odpowiadały. Na przykład klucze przychodzące muszą być zgodne z kluczami wychodzącymi zdalnego systemu, gdyż w przeciwnym razie połączenie nie powiedzie się.

W połączeniach ręcznych używane są klucze statyczne, które nie są odświeżane ani zmieniane w czasie, gdy połączenie jest aktywne. Aby zmienić klucz powiązany z połączeniem ręcznym, należy je zakończyć. Jeśli w danej sytuacji powyższe czynniki zagrażają bezpieczeństwu i obydwie strony połączenia obsługują protokół IKE (Internet Key Exchange), zamiast połączenia ręcznego można skonfigurować połączenie dynamiczne.

Aby zdefiniować właściwości połączenia ręcznego, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**.
2. Prawym przyciskiem myszy kliknij pozycję **Wszystkie połączenia** i wybierz opcję **Nowe połączenie ręczne**.
3. Wypełnij wszystkie arkusze właściwości. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Kliknij **OK**, aby zapisać wprowadzone zmiany.

**Uwaga:** W większości wypadków należy umożliwić interfejsowi VPN automatyczne wygenerowanie reguł pakietów, wybierając na stronie **Połączenie ręczne - Połączenie** opcję **Generuj filtr zgodny z punktem końcowym danych**. Jeśli jednak wybrana zostanie opcja **Reguła filtrowania strategii zostanie zdefiniowana w regule pakietów**, trzeba będzie następnie samodzielnie “Konfigurowanie reguły filtrowania strategii” na stronie 42.

## **Konfigurowanie reguł pakietów VPN**

Podczas tworzenia pierwszego połączenia należy pozwolić interfejsowi VPN na automatyczne wygenerowanie reguł pakietów VPN. Można to zrobić korzystając z Kreatora nowego połączenia lub ze stron właściwości połączenia VPN.

Jeśli reguły pakietów VPN będą utworzone za pomocą Edytora reguł w programie iSeries<sup>(TM)</sup> Navigator, w taki sam sposób należy utworzyć także wszelkie dodatkowe reguły. I odwrotnie, jeśli reguły filtrowania strategii zostały wygenerowane przez interfejs VPN, także wszystkie dodatkowe reguły filtrowania należy utworzyć w ten sam sposób.



Połączenia VPN wymagają zazwyczaj dwóch rodzajów reguł filtrowania: reguł typu Pre-IPSec i reguł filtrowania strategii. W poniższych sekcjach opisano sposób konfigurowania tych reguł za pomocą Edytora reguł pakietów w programie iSeries Navigator. Aby uzyskać informacje na temat innych opcji połączeń VPN i filtrowania, zapoznaj się z sekcją “Sieci VPN i filtrowanie IP” na stronie 29 w artykule poświęconym koncepcjom połączeń VPN.

- “Konfigurowanie reguły filtrowania typu Pre-IPSec”

Reguły typu Pre-IPSec to wszystkie reguły w systemie, które są uwzględniane przed regułami z czynnością typu IPSEC. W tej sekcji omówiono tylko takie reguły typu Pre-IPSec, których połączenie VPN wymaga do prawidłowego działania. W tym przypadku reguły typu Pre-IPSec to pary reguł umożliwiające przetwarzanie protokołu IKE podczas połączenia. Dzięki protokołowi IKE możliwe jest dynamiczne generowanie i negocjowanie kluczy podczas połączenia. Zależnie od danego środowiska i przyjętej strategii ochrony konieczne może być dodanie innych reguł typu Pre-IPSec.

**Uwaga:** Tego rodzaju reguły Pre-IPSec należy skonfigurować tylko wtedy, gdy zostały już zdefiniowane inne reguły umożliwiające przetwarzanie IKE dla konkretnych systemów. Jeśli jednak w systemie nie ma reguł filtrowania, które dopuszczałyby ruch danych IKE, wówczas zezwolenie na taki ruch ma charakter niejawnny.

- “Konfigurowanie reguły filtrowania strategii” na stronie 42

Reguła filtrowania strategii definiuje ruch danych, który może korzystać z połączenia VPN, oraz strategię ochrony danych, która będzie stosowana dla tego ruchu.

### Uwagi wstępne

Po dodaniu reguł filtrowania do interfejsu system automatycznie doda domyślną regułę DENY dla tego interfejsu. Oznacza to, że każdy rodzaj ruchu, który nie jest dopuszczony w sposób jawny, zostanie zablokowany. Reguła ta jest niewidoczna i nie można jej zmienić. W rezultacie może okazać się, że transmisja danych, która do tej pory przebiegała bez zakłóceń, jest z niewiadomych przyczyn blokowana po uaktywnieniu reguł filtrowania VPN. Aby umożliwić przesyłanie danym interfejsem ruchu innego niż VPN, należy dodać dla tego ruchu jawną regułę PERMIT.

Po skonfigurowaniu odpowiednich reguł filtrowania należy “Definiowanie interfejsu dla reguł filtrowania VPN” na stronie 43, do którego będą one stosowane, a następnie “Uaktywnianie reguł pakietów VPN” na stronie 44 je.

Poprawne skonfigurowanie reguł filtrowania ma zasadnicze znaczenie. W przeciwnym razie mogą one zablokować cały ruch IP przychodzący do serwera iSeries i wychodzący z niego. Dotyczyć to będzie także połączenia z programem iSeries Navigator, używanego do konfigurowania reguł filtrowania.

Jeśli reguły filtrowania nie zezwolą na ruch danych programu iSeries Navigator, program ten nie będzie mógł komunikować się z serwerem iSeries. Jeśli zaistnieje taka sytuacja, jedynym wyjściem będzie zalogowanie się do serwera iSeries przy użyciu interfejsu, który w dalszym ciągu umożliwia łączność, na przykład poprzez konsolę operacyjną. Aby usunąć wszystkie filtry w systemie, należy użyć komendy RMVTCPTBL. Komenda ta zakończy jednocześnie pracę wszystkich serwerów \*VPN i ponownie je uruchomi. Następnie należy skonfigurować filtry i ponownie je uaktywnić.

### Konfigurowanie reguły filtrowania typu Pre-IPSec

**Uwaga:** Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguł filtrowania strategii przez VPN.

Para serwerów protokołu IKE (Internet Key Exchange) dynamicznie negocjuje i odświeża klucze. Protokół IKE korzysta zwykle z portu 500. Aby umożliwić prawidłowe działanie protokołu IKE, należy pozwolić na przesyłanie przez port 500 datagramów UDP dla tego ruchu IP. W tym celu należy utworzyć parę reguł filtrowania; jedną dla ruchu przychodzącego i jedną dla ruchu wychodzącego, dzięki temu podczas połączenia możliwe będzie dynamiczne negocjowanie kluczy chroniących to połączenie:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Edytor reguł**. Spowoduje to utworzenie Edytora reguł pakietów, który umożliwi utworzenie lub edycję filtra i reguł translacji NAT dla danego serwera iSeries.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz **Wstaw** → **Filtr**.

5. Na stronie **Ogólne** określ nazwę zestawu filtrów VPN. Zaleca się utworzenie przynajmniej trzech różnych zestawów: jednego dla reguł filtrowania typu Pre-IPSec, jednego dla reguł filtrowania strategii i jednego dla różnych reguł filtrowania typu PERMIT i DENY. Nazwij zestaw zawierający reguły filtrowania typu pre-IPSec tak, aby nazwa zaczynała się od przedrostka *preipsec*. Na przykład *preipsecfilters*.
6. Z rozwijanej listy w polu **Akcja** wybierz **PERMIT**.
7. Z rozwijanej listy w polu **Kierunek** wybierz **OUTBOUND**.
8. Z rozwijanej listy w polu **Nazwa adresu źródłowego** wybierz **=**, a następnie w polu obok wpisz adres IP lokalnego serwera kluczy. Adres IP lokalnego serwera kluczy został określony w strategii protokołu IKE.
9. Z rozwijanej listy w polu **Nazwa adresu docelowego** wybierz **=**, a następnie w polu obok wpisz adres IP zdalnego serwera kluczy. Adres IP zdalnego serwera kluczy również został określony w strategii protokołu IKE.
10. Na stronie **Usługi** wybierz opcję **Usługa**. Spowoduje to udostępnienie pól **Protokół**, **Port źródłowy** i **Port docelowy**.
11. Z rozwijanej listy w polu **Protokół** wybierz **UDP**.
12. W pozycji **Port źródłowy** wybierz **=** w pierwszym polu i wpisz 500 w polu obok.
13. Powtórz powyższą czynność dla pola **Port docelowy**.
14. Kliknij przycisk **OK**.
15. Powtórz powyższe czynności, aby skonfigurować filtr dla kierunku INBOUND. Użyj tej samej nazwy zestawu i odpowiednio zmień wartości adresów IP.

**Uwaga:** Mniej bezpieczną, ale łatwiejszą opcją dopuszczania ruchu IKE przez połączenie jest skonfigurowanie tylko jednego filtra typu Pre-IPSec i użycie znaku zastępczego (\*) w polach **Kierunek**, **Nazwa adresu źródłowego** i **Nazwa adresu docelowego**.

Następnym krokiem jest “Konfigurowanie reguły filtrowania strategii” w celu określenia ruchu IP, który będzie chroniony przez połączenie VPN.

## Konfigurowanie reguły filtrowania strategii

**Uwaga:** Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguły filtrowania strategii przez VPN.

Reguła filtrowania strategii (reguła w której akcja=IPSEC) definiuje adresy, protokoły i porty, które mogą korzystać z połączenia VPN. Określa ona także strategię, która zostanie zastosowana do ruchu w połączeniu VPN. Aby skonfigurować regułę filtrowania strategii, wykonaj następujące czynności:

**Uwaga:** Jeśli właśnie skonfigurowano regułę typu Pre-IPSec (tylko dla połączeń dynamicznych), Edytor reguł pakietów będzie w dalszym ciągu otwarty. W takim wypadku należy przejść do punktu 4.

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Edytor reguł**. Spowoduje to otwarcie Edytora reguł pakietów, który umożliwi utworzenie lub edycję filtra i reguł translacji NAT dla danego serwera iSeries.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz **Wstaw** → **Filtr**.
5. Na stronie **Ogólne** określ nazwę zestawu filtrów VPN. Zaleca się utworzenie przynajmniej trzech różnych zestawów: jednego dla reguł filtrowania typu Pre-IPSec, jednego dla reguł filtrowania strategii i jednego dla różnych reguł filtrowania typu PERMIT i DENY. Na przykład *policyfilters*.
6. Z rozwijanej listy w polu **Akcja** wybierz **IPSEC**. Pole **Kierunek** ma wartość domyślną **OUTBOUND** i nie można tego zmienić. Pomimo tego w rzeczywistości odnosi się ono do ruchu dwukierunkowego. Wartość **OUTBOUND** jest wyświetlana, aby poprawić czytelność znaczenia wartości wejściowych. Na przykład wartości źródłowe są wartościami lokalnymi, a wartości docelowe wartościami zdalnymi.
7. W pozycji **Nazwa adresu źródłowego** wybierz **=** w pierwszym polu, a następnie wpisz adres IP lokalnego punktu końcowego danych w drugim polu. Można także określić zakres adresów IP lub adres IP z maską podsieci po zdefiniowaniu ich przy użyciu funkcji **Definiuj adresy**.

8. W pozycji **Nazwa adresu docelowego** wybierz = w pierwszym polu, a następnie wpisz adres IP zdalnego punktu końcowego danych w drugim polu. Można także określić zakres adresów IP lub adres IP z maską podsieci po zdefiniowaniu ich przy użyciu funkcji **Definiuj adresy**.
9. W polu **Kronikowanie** określ wymagany poziom kronikowania.
10. W polu **Nazwa połączenia** wybierz definicję połączenia, do którego będą stosowane te reguły filtrowania.
11. (opcjonalnie) Wpisz opis.
12. Na stronie **Usługi** wybierz opcję **Usługa**. Spowoduje to udostępnienie pól **Protokół, Port źródłowy i Port docelowy**.
13. W polach **Protokół, Port źródłowy i Port docelowy** wybierz wartości odpowiednie dla danego ruchu. Można także wybrać gwiazdkę (\*) z rozwijanej listy. Umożliwi to dowolnemu protokołowi korzystanie z połączenia VPN poprzez dowolny port.
14. Kliknij przycisk **OK**.

Następnym krokiem jest "Definiowanie interfejsu dla reguł filtrowania VPN", do którego zostaną zastosowane te reguły filtrowania.

**Uwaga:** Po dodaniu reguł filtrowania dla interfejsu system automatycznie doda domyślną regułę DENY dla tego interfejsu. Oznacza to, że każdy rodzaj ruchu, który nie jest dopuszczony w sposób jawny, zostanie zablokowany. Reguła ta jest niewidoczna i nie można jej zmienić. W rezultacie może okazać się, że połączenia, które do tej pory działały prawidłowo, są z niewiadomych przyczyn blokowane po uaktywnieniu reguł filtrowania VPN. Aby umożliwić przesyłanie danym interfejsem ruchu innego niż VPN, należy dodać dla tego ruchu jawną regułę PERMIT.

## Definiowanie interfejsu dla reguł filtrowania VPN

Po skonfigurowaniu reguł pakietów i wszelkich innych reguł potrzebnych przy połączeniu VPN należy zdefiniować interfejs, do którego zostaną one zastosowane.

W celu zdefiniowania interfejsu, do którego zostaną zastosowane reguły filtrowania VPN, wykonaj następujące czynności:

**Uwaga:** Jeśli właśnie skonfigurowano reguły pakietów VPN, Edytor reguł pakietów będzie w dalszym ciągu otwarty. W takim wypadku należy przejść do kroku 4.

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Edytor reguł**. Spowoduje to otwarcie Edytora reguł pakietów, który umożliwi utworzenie lub edycję filtru i reguł translacji NAT dla danego serwera iSeries.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz **Wstaw** → **Interfejs filtru**.
5. Na stronie **Ogólne** wybierz opcję **Nazwa linii**, a następnie wybierz z rozwijanej listy opis linii, do której stosowane będą reguły pakietów VPN.
6. (opcjonalnie) Wpisz opis.
7. Na stronie **Zestawy filtrów** kliknij przycisk **Dodaj**, aby dodać nazwę każdego zestawu dla skonfigurowanych filtrów.
8. Kliknij przycisk **OK**.
9. Zapisz plik reguł. Plik zostanie zapisany w zintegrowanym systemie plików na serwerze iSeries z rozszerzeniem .i3p.

**Uwaga:** Nie należy zapisywać pliku w następującym katalogu:

/QIBM/UserData/OS400/TCPIP/RULEGEN

Katalog ten jest przeznaczony wyłącznie na użytek systemu. Jeśli kiedykolwiek pojawi się potrzeba użycia komendy RMVTCPTBL \*ALL, aby dezaktywować reguły pakietów, usunie ona wszystkie pliki znajdujące się w tym katalogu.

Po zdefiniowaniu interfejsu dla reguł pakietów należy je “Uaktywnianie reguł pakietów VPN”, aby można było uruchomić połączenie VPN.

## Uaktywnianie reguł pakietów VPN

Aby można było uruchomić połączenie VPN, należy najpierw uaktywnić reguły pakietów VPN. Jeśli w systemie są uruchomione połączenia VPN, nie można uaktywnić (ani dezaktywować) reguł pakietów. Dlatego przed uaktywnieniem reguł filtrowania VPN należy sprawdzić, czy żadne powiązane z nim połączenia nie są aktywne.

Jeśli połączenia VPN zostały utworzone za pomocą Kreatora nowego połączenia, można zdecydować się na automatyczne uaktywnienie reguł powiązanych z tymi połączeniami. Należy jednak pamiętać, że jeśli w systemie są aktywne inne reguły pakietów dla wybranych interfejsów, zostaną one zastąpione przez reguły filtrowania strategii VPN.

Jeśli reguły wygenerowane przez interfejs VPN mają być uaktywnione za pomocą Edytora reguł pakietów, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Uaktywnij**. Spowoduje to utworzenie okna dialogowego **Uaktywnij reguły pakietów**.
3. Wybierz uaktywnienie wyłącznie wygenerowanych reguł VPN, wyłącznie wybranego pliku lub zarówno wygenerowanych reguł VPN, jak i wybranego pliku. Można wybrać ostatnią opcję, aby na przykład wymusić na interfejsie różne reguły typu PERMIT i DENY, oprócz wygenerowanych reguł VPN.
4. Wybierz interfejs, dla którego chcesz uaktywnić reguły. Można wybrać określony interfejs, identyfikator typu punkt z punktem albo wszystkie interfejsy i wszystkie identyfikatory typu punkt z punktem.
5. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić zamiar weryfikacji i uaktywnienia reguł dla określonych interfejsów. Po kliknięciu przycisku OK system sprawdzi składniową i semantyczną poprawność reguł oraz wyświetli wyniki w oknie komunikatu u dołu edytora. W wypadku komunikatów o błędach dotyczących określonego pliku i numeru wiersza można kliknąć dany komunikat prawym przyciskiem myszy i wybrać opcję **Przejdź do wiersza**, aby wyróżnić błąd w pliku.

Po uaktywnieniu reguł filtrowania można “Uruchamianie połączenia VPN”.

## Uruchamianie połączenia VPN

W tej sekcji zakłada się, że połączenie VPN zostało skonfigurowane prawidłowo. Aby uruchomić połączenie VPN, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Jeśli serwer VPN nie jest uruchomiony, kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Uruchom**. Spowoduje to uruchomienie serwera sieci VPN.
3. Sprawdź, czy reguły pakietów zostały “Uaktywnianie reguł pakietów VPN”.
4. Rozwiń pozycję **Sieć VPN** → **Połączenia chronione**.
5. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
6. Prawym przyciskiem myszy kliknij połączenie, które chcesz uruchomić, i wybierz opcję **Uruchom**. Aby uruchomić kilka połączeń, zaznacz je wszystkie, kliknij prawym przyciskiem myszy i wybierz opcję **Uruchom**.

---

## Zarządzanie połączeniami VPN

Interfejs VPN dostępny w programie iSeries<sup>(TM)</sup> Navigator umożliwia obsługę wszystkich zadań administracyjnych, takich jak:

- “Uruchamianie połączenia VPN”  
Wykonanie opisanych w tej sekcji zadań pozwoli uruchomić połączenie inicjowane lokalnie.

- “Ustawianie domyślnych atrybutów połączeń”  
Wartości domyślne są wstępnie wstawiane do paneli wykorzystywanych podczas tworzenia nowych strategii i połączeń. Można je określić dla poziomów ochrony, zarządzania kluczem sesji, okresu ważności klucza i czasu trwania połączenia.
- “Resetowanie połączeń w wypadku wystąpienia błędu”  
Zresetowanie połączenia po wystąpieniu błędu powoduje przełączenie go w stan bezczynności.
- “Wyświetlanie informacji o błędach”  
Wykonanie opisanych w tej sekcji czynności pomoże określić przyczyny występowania błędów podczas połączeń.
- “Wyświetlanie atrybutów połączeń aktywnych” na stronie 46  
W tej sekcji opisano zadania umożliwiające sprawdzenie statusu i innych atrybutów połączeń aktywnych.
- “Korzystanie z programu do śledzenia serwera VPN” na stronie 46  
Program do śledzenia serwera VPN umożliwia skonfigurowanie, uruchomienie, zatrzymanie i wyświetlenie informacji o śledzeniu serwerów Menedżera połączeń VPN i VPN Key Manager. Narzędzie to jest podobne do komendy TRCTCPAPP \*VPN uruchamianej z interfejsu znakowego z tym, że pozwala wyświetlać informacje o śledzeniu w czasie, gdy połączenie jest aktywne.
- “Wyświetlanie protokołów zadań serwera VPN” na stronie 46  
W tej sekcji przedstawiono instrukcje dotyczące wyświetlania protokołów zadań VPN Key Manager i Menedżera połączeń VPN.
- “Zatrzymywanie połączeń VPN” na stronie 47  
Wykonanie opisanych w tej sekcji czynności spowoduje zatrzymanie aktywnych połączeń.
- “Wyświetlanie atrybutów powiązań Security Association (SA)” na stronie 47  
W sekcji opisano sposób wyświetlania atrybutów powiązań Security Association (SA) przypisanych aktywnemu połączeniu.
- “Usuwanie obiektów konfiguracyjnych VPN” na stronie 47  
Przed usunięciem obiektu konfiguracyjnego VPN z bazy danych strategii należy dokładnie rozważyć wpływ, jaki to będzie miało na inne połączenia i grupy połączeń.

## Ustawianie domyślnych atrybutów połączeń

Domyślne wartości ustawień ochrony są wstępnie wpisywane w różne pola podczas tworzenia nowych obiektów VPN.

Aby ustawić domyślne wartości atrybutów dla połączeń VPN, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Sieć VPN** i wybierz opcję **Domyślne**.
3. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
4. Po wypełnieniu wszystkich arkuszy właściwości kliknij przycisk **OK**.

## Resetowanie połączeń w wypadku wystąpienia błędu

Aby odświeżyć połączenie, w którym wystąpił błąd, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij połączenie, które chcesz zresetować, i wybierz opcję **Zresetuj**. Spowoduje to zresetowanie połączenia do stanu bezczynności. Aby zresetować kilka połączeń, w których wystąpił błąd, zaznacz je wszystkie, kliknij prawym przyciskiem myszy i wybierz opcję **Zresetuj**.

## Wyświetlanie informacji o błędach

Aby wyświetlić informacje o połączeniach, w których wystąpił błąd, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.



3. Prawym przyciskiem myszy kliknij połączenie z błędem, które chcesz wyświetlić, i wybierz opcję **Informacje o błędzie**.

## Wyświetlanie atrybutów połączeń aktywnych

Aby wyświetlić bieżące atrybuty połączenia aktywnego lub połączenia na żądanie, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij połączenie aktywne lub połączenie na żądanie, które chcesz wyświetlić i wybierz opcję **Właściwości**.
4. Przejdź do strony **Bieżące atrybuty**, aby wyświetlić atrybuty połączenia.

W oknie programu iSeries Navigator można również wyświetlić atrybuty wszystkich połączeń jednocześnie. Domyślnie wyświetlane są tylko takie atrybuty, jak Status, Opis i Typ połączenia. Wyświetlane dane można zmienić, wykonując następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**.
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Z menu **Obiekty** wybierz opcję **Kolumny**. Spowoduje to otwarcie okna dialogowego umożliwiającego wybór atrybutów, które mają być wyświetlane w oknie programu iSeries Navigator.




Należy pamiętać, że wprowadzone zmiany nie dotyczą wyłącznie danego użytkownika lub komputera PC, ale całego systemu.

## Korzystanie z programu do śledzenia serwera VPN

Aby wyświetlić informacje o śledzeniu serwera VPN, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Sieć VPN**, wybierz opcję **Narzędzia diagnostyczne**, a następnie **Śledzenie serwera**.

Aby określić typ informacji o śledzeniu generowanych przez VPN Key Manager i Menedżera połączeń VPN, wykonaj następujące czynności:

1. W oknie **Wirtualne sieci prywatne** kliknij ikonę  (Opcje).
2. Na stronie **Menedżer połączeń** określ, jaki typ śledzenia ma być generowany przez serwer Menedżera połączeń.
3. Na stronie **Key Manager** określ, jaki typ śledzenia ma być generowany przez serwer Key Manager.
4. Kliknij przycisk **Pomoc**, aby dowiedzieć się, jak wypełnić stronę lub dowolne z jej pól.
5. Kliknij **OK**, aby zapisać wprowadzone zmiany.
6. Kliknij ikonę  (Start), aby uruchomić śledzenie. Okresowo klikaj ikonę  (Odśwież), aby wyświetlić najnowsze informacje o śledzeniu.

## Wyświetlanie protokołów zadań serwera VPN

Aby wyświetlić bieżące protokoły zadań VPN Key Manager lub Menedżera połączeń VPN, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Sieć VPN** i wybierz opcję **Narzędzia diagnostyczne**, a następnie wybierz protokół zadania dowolnego serwera.



## Wyświetlanie atrybutów powiązań Security Association (SA)

Aby wyświetlić atrybuty Security Association (SA) przypisanych aktywnemu połączeniu, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij odpowiednie połączenie aktywne i wybierz opcję **Security Associations**. Spowoduje to otwarcie okna umożliwiającego wyświetlenie właściwości każdego powiązania SA przypisanego do konkretnego połączenia.

## Zatrzymywanie połączeń VPN

Aby zatrzymać połączenie aktywne lub połączenie na żądanie, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij połączenie, które chcesz zatrzymać, i wybierz opcję **Zatrzymaj**. Aby zatrzymać kilka połączeń, zaznacz je wszystkie, kliknij prawym przyciskiem myszy i wybierz opcję **Zatrzymaj**.

## Usuwanie obiektów konfiguracyjnych VPN

Jeśli konieczne jest usunięcie połączenia z bazy danych strategii VPN, wykonaj następujące czynności:

1. W programie iSeries<sup>(TM)</sup> Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij połączenie, które chcesz usunąć i wybierz opcję **Usuń**.

---

## Rozwiązywanie problemów dotyczących połączeń VPN

VPN to skomplikowana i szybko zmieniająca się technologia, która wymaga przynajmniej podstawowej znajomości technologii standardu IPsec. Konieczna jest także znajomość reguł pakietów IP, ponieważ połączenia VPN wymagają do prawidłowego działania kilku reguł filtrowania. Z uwagi na ten poziom złożoności, od czasu do czasu mogą zdarzać się problemy związane z połączeniami VPN. Rozwiązywanie problemów dotyczących połączeń VPN nie zawsze jest łatwe. Należy dokładnie poznać system i środowisko sieciowe, a także komponenty wykorzystywane do zarządzania nim. W wymienionych poniżej sekcjach przedstawiono wskazówki przydatne do rozwiązywania różnych problemów, które mogą wystąpić podczas korzystania z połączeń VPN:

- “Wprowadzenie do rozwiązywania problemów dotyczących połączeń VPN” na stronie 48  
W sekcji tej przedstawiono podstawowe informacje dotyczące znajdowania i usuwania przyczyn problemów dotyczących połączeń.
- “Typowe błędy konfiguracyjne i sposoby ich usuwania” na stronie 49  
W tej sekcji opisano najczęściej występujące błędy powodowane przez użytkowników oraz możliwe ich rozwiązania.
- “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QIPFILTER” na stronie 54  
Ta sekcja zawiera informacje dotyczące reguł filtrowania VPN.
- “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QVPN” na stronie 57  
W tej sekcji przedstawiono informacje o ruchu IP i połączeniach.
- “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą protokołów zadań VPN” na stronie 59  
W tej sekcji opisano różne protokoły zadań wykorzystywane przez połączenia VPN.
- “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą śledzenia komunikacji w systemie OS/400” na stronie 65  
W sekcji opisano sposób śledzenia danych przesyłanych linią komunikacyjną.

# Wprowadzenie do rozwiązywania problemów dotyczących połączeń VPN

Do analizowania problemów dotyczących połączeń VPN można przystąpić na kilka sposobów:

1. Sprawdź, czy zastosowano najnowsze poprawki PTF.
2. Sprawdź, czy zostały spełnione minimalne “Wymagania konfiguracyjne VPN” na stronie 31.
3. Przejrzyj wszystkie komunikaty o błędach znalezione w oknie “Wyświetlanie informacji o błędach” na stronie 45 lub w “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą protokołów zadań VPN” na stronie 59, zarówno dla systemu zdalnego, jak i lokalnego. W trakcie rozwiązywania problemów dotyczących połączeń VPN często konieczne jest sprawdzenie obydwu końców połączenia. Należy ponadto uwzględnić konieczność sprawdzenia czterech adresów: lokalnego i zdalnego punktu połączenia, czyli adresów, w których do pakietów IP stosowany jest protokół IPSec, oraz lokalnego i zdalnego punktu końcowego danych, czyli źródłowego i docelowego adresu pakietu IP.
4. Jeśli w znalezionych komunikatach o błędach nie będzie informacji, które pozwoliłyby rozwiązać problem, sprawdź kronikę “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QIPFILTER” na stronie 54.
5. “Rozwiązywanie problemów dotyczących połączeń VPN za pomocą śledzenia komunikacji w systemie OS/400” na stronie 65 na serwerze iSeries<sup>(TM)</sup> to kolejne miejsce, w którym można znaleźć ogólne informacje o tym, czy system lokalny odbiera lub wysyła żądania.
6. Komenda Śledzenie aplikacji TCP/IP (Trace TCP Application - TRCTCPAPP) udostępnia następujący sposób zlokalizowania problemu. Serwis IBM<sup>(R)</sup> używa najczęściej komendy TRCTCPAPP do uzyskania danych wyjściowych śledzenia w celu analizy problemów dotyczących połączenia.

## Sprawdzenie innych elementów

Jeśli błąd pojawia się po skonfigurowaniu połączenia i nie wiadomo, w którym miejscu sieci go szukać, należy spróbować uprościć lokalne środowisko sieciowe. Zamiast na przykład badać wszystkie części połączenia VPN jednocześnie, należy zacząć od samego połączenia IP. Poniższa lista przedstawia podstawowe etapy analizy problemu dotyczącego połączenia VPN, od najprostszego połączenia IP do bardziej złożonego połączenia VPN:

1. Zaczynj od konfiguracji IP pomiędzy lokalnym i zdalnym hostem. Usuń wszystkie filtry IP z interfejsu wykorzystywanego do komunikacji przez obydwa systemy. Czy można pomyślnie wykonać komendę PING z hosta lokalnego do zdalnego?

**Uwaga:** Należy pamiętać o podpowiedziach komendy PING; wpisać adres zdalnego systemu i użyć klawisza PF10 do wprowadzenia dodatkowych parametrów, a następnie wpisać lokalny adres IP. Ma to szczególne znaczenie w wypadku wielu interfejsów fizycznych lub logicznych. Dzięki temu w pakietach komendy PING zamieszczone będą odpowiednie adresy.

Jeśli odpowiedź brzmi **tak**, przejdź do punktu 2. Jeśli **nie**, sprawdź konfigurację IP, status interfejsu i pozycje routingu. W wypadku prawidłowej konfiguracji, należy sprawdzić za pomocą śledzenia komunikacji, czy na przykład żądanie komendy PING wychodzi z systemu. Brak odpowiedzi na żądanie PING oznacza, że problem tkwi w ustawieniach sieci lub zdalnego systemu.

**Uwaga:** W sieci mogą istnieć pośrednie routery lub firewalle, które filtrują pakiety IP, w tym również pakiety komendy PING. Komenda PING wykorzystuje zwykle protokół ICMP. Jeśli wykonanie komendy PING powiedzie się, oznacza to, że łączność funkcjonuje poprawnie. W przeciwnym razie nie wiadomo nic poza tym, że wykonanie komendy PING nie powiodło się. Do sprawdzenia łączności pomiędzy obydwojema systemami można użyć innych protokołów IP, takich jak Telnet lub FTP.

2. Sprawdź, czy reguły filtrowania dla połączenia VPN zostały uaktywnione. Czy filtrowanie uruchamia się prawidłowo? Jeśli odpowiedź brzmi **tak**, przejdź do punktu 3. Jeśli **nie**, sprawdź komunikaty w oknie Reguły pakietów w programie iSeries Navigator. Sprawdź, czy reguły filtrowania nie włączają translacji NAT (Network Address Translation) dla ruchu VPN.
3. “Uruchamianie połączenia VPN” na stronie 44. Czy połączenie uruchamia się prawidłowo? Jeśli odpowiedź brzmi **tak**, przejdź do punktu 4. Jeśli **nie**, sprawdź błędy w protokołach zadań QTOVMAN i QTOKVPIKE. Aby można było korzystać z połączeń VPN, dostawca ISP (Internet Service Provider) i każda brama ochrony w

lokalnej sieci muszą obsługiwać protokoły AH (Authentication Header) i ESP (Encapsulated Security Payload). To, czy używany jest protokół AH, czy ESP zależy od właściwości zdefiniowanych dla połączenia VPN.

4. Czy można uaktywnić sesję użytkownika w połączeniu VPN? Jeśli odpowiedź brzmi **tak**, połączenie VPN działa prawidłowo. Jeśli **nie**, sprawdź, czy reguły pakietów oraz grupy z kluczem dynamicznym i połączenia VPN nie zawierają reguł filtrowania blokujących wymagany ruch danych użytkownika.

## Typowe błędy konfiguracyjne i sposoby ich usuwania

W tej sekcji opisano niektóre z częściej występujących problemów dotyczących połączeń VPN oraz zamieszczono odsyłacze do wskazówek pomocnych przy rozwiązywaniu tych problemów.

**Uwaga:** Konfigurowanie połączenia to w rzeczywistości tworzenie kilku różnych obiektów konfiguracyjnych, z których każdy jest niezbędny do nawiązania połączenia VPN. Według terminów z interfejsu GUI VPN obiekty te to: Strategie ochrony IP oraz Połączenia chronione. Tym samym, kiedy przedstawione tu informacje odwołują się do obiektu, chodzi o taki element połączenia VPN lub kilka takich elementów.

### Często spotykane komunikaty o błędach

#### Komunikat

“Komunikat o błędzie połączenia VPN: TCP5B28” na stronie 50

#### Objaw

Przy próbie uaktywnienia reguł filtrowania dla interfejsu wyświetlany jest komunikat: TCP5B28 Naruszenie kolejności CONNECTION\_DEFINITION

“Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji” na stronie 50

Po kliknięciu prawym przyciskiem myszy obiektu VPN i wybraniu opcji **Właściwości** lub **Usuń** wyświetlany jest komunikat **Nie można znaleźć pozycji**.

“Komunikat o błędzie połączenia VPN: NIEOPRAWNY PARAMETR PINBUF” na stronie 51

Podczas próby uruchomienia połączenia wyświetlany jest komunikat **NIEOPRAWNY PARAMETR PINBUF...**

“Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji, Zdalny serwer kluczy...” na stronie 51

Po wybraniu opcji **Właściwości** dla połączenia z kluczem dynamicznym wyświetlany jest komunikat o błędzie z informacją, że serwer nie może odnaleźć podanego zdalnego serwera kluczy.

“Komunikat o błędzie połączenia VPN: Nie można zaktualizować obiektu” na stronie 52

Po kliknięciu przycisku **OK** na arkuszu właściwości grupy z kluczem dynamicznym lub połączenia ręcznego wyświetlany jest komunikat z informacją, że system nie może zaktualizować obiektu.

“Komunikat o błędzie połączenia VPN: Nie można zaszyfrować klucza...” na stronie 52

Wyświetlany jest komunikat informujący, że system nie może zaszyfrować kluczy, ponieważ wartość QRETSVRSEC musi być równa 1.

“Komunikat o błędzie połączenia VPN: CPF9821” na stronie 53

Podczas próby otworzenia lub rozwinięcia pojemnika Strategie IP w programie iSeries<sup>(TM)</sup> Navigator wyświetlany jest komunikat CPF9821 - Brak uprawnień do programu QTFRPRS w bibliotece QSYS.

### Inne problemy, które mogą wystąpić

#### Błąd

“Błąd połączenia VPN: Wszystkie klucze są puste” na stronie 53

#### Objaw

Podczas wyświetlania właściwości połączenia ręcznego wszystkie wstępne klucze współużytkowane i klucze algorytmów dla połączenia są puste.

“Błąd połączenia VPN: Wyświetlenie ekranu wpisania się do innego systemu podczas korzystania z Edytora reguł pakietów” na stronie 53

Przy pierwszej próbie skorzystania z interfejsu Reguły pakietów w programie iSeries Navigator wyświetlany jest ekran wpisania się do systemu innego niż system bieżący.

“Błąd połączenia VPN: Pusty status połączenia w oknie programu iSeries Navigator” na stronie 53

W kolumnie **Status** w oknie programu iSeries Navigator nie ma wartości dla połączenia.

“Błąd połączenia VPN: Po zatrzymaniu połączenie ma status Włączone” na stronie 53

Po zatrzymaniu połączenia jest ono w dalszym ciągu wyświetlane jako aktywne w oknie programu iSeries Navigator.

“Błąd połączenia VPN: Nie można wybrać algorytmu szyfrowania 3DES” na stronie 54

Podczas pracy z transformacjami strategii IKE lub połączeniem ręcznym algorytm szyfrowania 3DES jest niedostępny.

“Błąd połączenia VPN: W oknie programu iSeries Navigator wyświetlane są nieoczekiwane kolumny” na stronie 54

Skonfigurowano kolumny, które mają być wyświetlane w oknie programu iSeries Navigator dla połączeń VPN, ale później wyświetlane są inne kolumny.

“Błąd połączenia VPN: Nie można dezaktywować aktywnych reguł filtrowania” na stronie 54

Podczas próby dezaktywacji bieżącego zestawu reguł filtrowania w oknie wyników wyświetlany jest komunikat **Nie można dezaktywować aktywnych reguł**.

“Błąd połączenia VPN: Zmiana grupy z kluczem dynamicznym dla połączenia” na stronie 54

Podczas tworzenia połączenia z kluczem dynamicznym określono grupę z kluczem dynamicznym i identyfikator zdalnego serwera kluczy. Później, podczas przeglądania właściwości powiązanego obiektu połączenia, na stronie Ogólne arkusza właściwości wyświetlany jest ten sam identyfikator zdalnego serwera kluczy, ale inna grupa z kluczem dynamicznym.

## Komunikat o błędzie połączenia VPN: TCP5B28

### Objaw:

W trakcie próby uaktywnienia reguł filtrowania dla interfejsu wyświetlany jest następujący komunikat:

TCP5B28: Naruszenie kolejności CONNECTION\_DEFINITION

### Możliwe rozwiązanie:

Próbowano uaktywnić reguły filtrowania z definicjami połączenia, które były uporządkowane w innej kolejności niż zestaw reguł uaktywniony poprzednio. Najprostszym sposobem korekty tego błędu jest uaktywnienie reguł filtrowania dla **wszystkich interfejsów** zamiast dla indywidualnego interfejsu.

## Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji

### Objaw:

Po kliknięciu prawym przyciskiem obiektu w oknie Wirtualne sieci prywatne i wybraniu opcji **Właściwości** lub **Usuń** wyświetlany jest następujący komunikat:



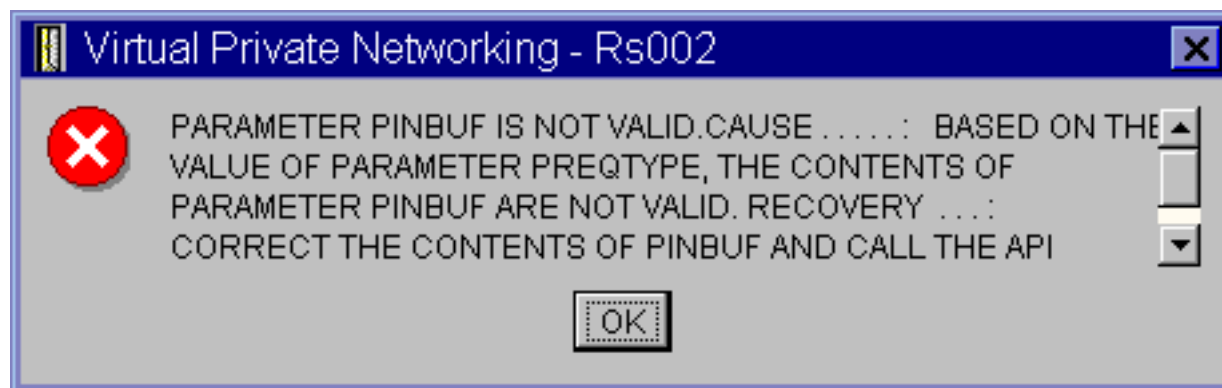
### Możliwe rozwiązanie:

- Być może obiekt został usunięty lub zmieniono nazwę obiektu i jeszcze nie odświeżono zawartości okna. W rezultacie obiekt jest w dalszym ciągu wyświetlany w oknie Wirtualne sieci prywatne. Aby sprawdzić, czy tak jest faktycznie, z menu **Widok** wybierz opcję **Odśwież**. Jeśli obiekt jest w dalszym ciągu wyświetlany w oknie Wirtualne sieci prywatne, przejdź do następnego punktu.
- Podczas konfigurowania właściwości obiektu mógł wystąpić błąd komunikacji pomiędzy serwerem VPN a serwerem iSeries<sup>(TM)</sup>. Wiele obiektów wyświetlanych w oknie Wirtualne sieci prywatne odnosi się do więcej niż jednego obiektu w bazie danych strategii VPN. Tym samym błąd komunikacji mógł spowodować, że niektóre z obiektów w bazie danych w dalszym ciągu odnoszą się do obiektu w oknie Wirtualne sieci prywatne. Zawsze kiedy podczas tworzenia lub aktualizowania obiektu nastąpi utrata synchronizacji, jest wyświetlany komunikat o błędzie. Jedynym sposobem rozwiązania tego problemu jest kliknięcie przycisku **OK** w oknie komunikatu. Spowoduje to otworenie arkusza właściwości obiektu, dla którego wystąpił błąd. Tylko pole nazwy w arkuszu właściwości będzie miało wartość. Wszystkie pozostałe pola będą puste (lub będą zawierać wartości domyślne). Wpisz poprawne atrybuty obiektu i kliknij przycisk **OK**, aby zapisać zmiany.
- Podobny błąd występuje podczas próby usunięcia obiektu. Aby rozwiązać ten problem, należy wypełnić pusty arkusz właściwości, wyświetlony po kliknięciu przycisku **OK** w oknie komunikatu o błędzie. Spowoduje to aktualizację wszelkich łącz z bazą danych strategii VPN, które zostały zerwane. Dzięki temu będzie można usunąć obiekt.

### Komunikat o błędzie połączenia VPN: NIEPOPRAWNY PARAMETR PINBUF

#### Objaw:

Podczas próby uruchomienia połączenia wyświetlany jest następujący komunikat:



#### Możliwe rozwiązanie:

Sytuacja taka zdarza się, kiedy dany system używa ustawień narodowych, dla których małe litery nie są odwzorowywane prawidłowo. Aby poprawić ten błąd, należy sprawdzić, czy wszystkie obiekty używają tylko wielkich liter lub zmienić ustawienia narodowe systemu.

### Komunikat o błędzie połączenia VPN: Nie można znaleźć pozycji, Zdalny serwer kluczy...

#### Objaw:

Po wybraniu opcji **Właściwości** dla połączenia z kluczem dynamicznym wyświetlany jest komunikat podobny do poniższego:



**Możliwe rozwiązanie:**

Błąd ten pojawia się, gdy utworzy się połączenie ze zdalnym serwerem kluczy o określonym identyfikatorze, a następnie ten zdalny serwer kluczy zostanie usunięty ze swojej grupy z kluczem dynamicznym. W celu usunięcia tego błędu, należy kliknąć przycisk **OK** w oknie komunikatu o błędzie. Spowoduje to otwarcie arkusza właściwości dla połączenia z kluczem dynamicznym, w którym wystąpił błąd. W arkuszu tym należy na powrót dodać zdalny serwer kluczy do grupy z kluczem dynamicznym lub wybrać identyfikator innego zdalnego serwera kluczy. Następnie należy kliknąć przycisk **OK** w arkuszu właściwości, aby zapisać zmiany.

**Komunikat o błędzie połączenia VPN: Nie można zaktualizować obiektu**

**Objaw:**

Po kliknięciu przycisku **OK** na arkuszu właściwości grupy z kluczem dynamicznym lub połączenia ręcznego wyświetlany jest następujący komunikat:



**Możliwe rozwiązanie:**

Błąd ten pojawia się podczas próby zmiany obiektu używanego przez aktywne połączenie. Nie można zmienić obiektu należącego do aktywnego połączenia. Aby zmienić obiekt, należy zidentyfikować odpowiednie połączenie aktywne, kliknąć je prawym przyciskiem myszy i wybrać opcję **Zatrzymaj** z menu kontekstowego.

**Komunikat o błędzie połączenia VPN: Nie można zaszyfrować klucza...**

**Objaw:**

Wyświetlany jest następujący komunikat o błędzie:





**Możliwe rozwiązanie:**

QRETSVRSEC to wartość systemowa wskazująca, czy w systemie mogą być przechowywane zaszyfrowane klucze. Jeśli wartość ta wynosi 0, oznacza to, że w bazie strategii VPN nie można przechowywać wstępnych kluczy współużytkowanych ani kluczy algorytmów dla połączenia ręcznego. Aby rozwiązać ten problem, należy połączyć się z systemem w trybie emulacji sesji terminalu 5250. W wierszu komend należy wpisać `wrksysval` i nacisnąć klawisz **Enter**. Na wyświetlonej liście należy odszukać wartość QRETSVRSEC i wpisać obok niej 2 (zmiana). Na następnym panelu należy wpisać 1 i nacisnąć klawisz **Enter**.

**Komunikat o błędzie połączenia VPN: CPF9821****Objaw:**

Podczas próby rozwinięcia pojemnika Strategie IP w programie iSeries<sup>(TM)</sup> wyświetlany jest komunikat CPF9821- Brak uprawnień do programu QTFRPRS w bibliotece QSYS.

**Możliwe rozwiązanie:**

Przyczyną błędu może być brak wymaganych uprawnień do pobierania bieżącego statusu Reguł pakietów lub Menedżera połączeń VPN. Sprawdź, czy masz uprawnienie \*IOSYSCFG do dostępu do funkcji Reguły pakietów w programie iSeries Navigator.

**Błąd połączenia VPN: Wszystkie klucze są puste****Objaw:**

Wszystkie wstępne klucze współużytkowane i klucze algorytmów dla połączeń ręcznych są puste.

**Możliwe rozwiązanie:**

Sytuacja taka zdarza się, gdy wartość systemowa QRETSVRSEC zostanie ustawiona z powrotem na 0. Powoduje to usunięcie wszystkich kluczy z bazy danych strategii VPN. Aby usunąć ten błąd, należy ustawić tę wartość systemową na 1, a następnie ponownie wprowadzić wszystkie klucze. Opis tej czynności zawiera sekcja “Komunikat o błędzie połączenia VPN: Nie można zaszyfrować klucza...” na stronie 52.

**Błąd połączenia VPN: Wyświetlenie ekranu wpisania się do innego systemu podczas korzystania z Edytora reguł pakietów****Objaw:**

Przy pierwszej próbie skorzystania z interfejsu Reguły pakietów wyświetlany jest ekran wpisania się do systemu innego niż system bieżący.

**Możliwe rozwiązanie:**

Edytor reguł pakietów przechowuje reguły ochrony pakietów w zintegrowanym systemie plików, wykorzystując kod Unicode. Dodatkowy ekran wpisania się pozwala programowi iSeries<sup>(TM)</sup> Access uzyskać odpowiednią tabelę konwersji dla kodu Unicode. Sytuacja taka zdarza się tylko raz.

**Błąd połączenia VPN: Pusty status połączenia w oknie programu iSeries Navigator****Objaw:**

W kolumnie **Status** w oknie programu iSeries<sup>(TM)</sup> Navigator nie ma wartości dla połączenia.

**Możliwe rozwiązanie:**

Brak wartości statusu wskazuje, że połączenie jest w trakcie uruchamiania. To znaczy, że jeszcze nie działa, ale oznacza też, że jeszcze nie wystąpił błąd. Po odświeżeniu zawartości okna dla połączenia będzie wyświetlany jeden z następujących statusów: **Błąd**, **Włączone**, **Na żądanie** lub **Bezczynne**.

**Błąd połączenia VPN: Po zatrzymaniu połączenie ma status Włączone****Objaw:**

Po zatrzymaniu połączenia, w oknie programu iSeries<sup>(TM)</sup> jest ono nadal widoczne jako aktywne.

**Możliwe rozwiązanie:**

Typową przyczyną takiej sytuacji jest nieodświeżenie okna programu iSeries Navigator. Tym samym w oknie wyświetlane są nieaktualne informacje. Aby rozwiązać ten problem, należy wybrać opcję **Odśwież** z menu **Widok**.

## Błąd połączenia VPN: Nie można wybrać algorytmu szyfrowania 3DES

### Objaw:

Podczas pracy z transformacjami strategii IKE lub połączeniem ręcznym algorytm szyfrowania 3DES jest niedostępny.

### Możliwe rozwiązanie:

Najprawdopodobniej w systemie zainstalowany jest tylko produkt Cryptographic Access Provider AC2 (5722-AC2), a nie produkt Cryptographic Access Provider AC3 (5722-AC3). Wersja AC2 umożliwia stosowanie wyłącznie algorytmu szyfrowania Data Encryption Standard (DES) z uwagi na ograniczenia długości klucza.

## Błąd połączenia VPN: W oknie programu iSeries Navigator wyświetlane są nieoczekiwane kolumny

### Objaw:

Skonfigurowano kolumny, które mają być wyświetlane w oknie programu iSeries Navigator dla połączeń VPN, ale później wyświetlane są inne kolumny.

### Możliwe rozwiązanie:

Kiedy zmienia się kolumny, które mają zostać wyświetlone, wprowadzone zmiany nie dotyczą wyłącznie danego użytkownika lub komputera PC, ale całego systemu. Kiedy zatem jeden z użytkowników zmieni kolumny w oknie, będzie to miało wpływ na wyświetlanie wszystkich połączeń w systemie.

## Błąd połączenia VPN: Nie można dezaktywować aktywnych reguł filtrowania

### Objaw:

Podczas próby dezaktywacji bieżącego zestawu reguł filtrowania w oknie wyników wyświetlany jest komunikat Nie można dezaktywować aktywnych reguł.

### Możliwe rozwiązanie:

Najczęściej ten komunikat o błędzie oznacza, że istnieje przynajmniej jedno aktywne połączenie VPN. Należy zatrzymać wszystkie połączenia o statusie **włączone**. W tym celu trzeba kliknąć prawym przyciskiem myszy każde aktywne połączenie i wybrać opcję **Zatrzymaj**. Teraz można dezaktywować reguły filtrowania.

## Błąd połączenia VPN: Zmiana grupy z kluczem dynamicznym dla połączenia

### Objaw:

Podczas tworzenia połączenia z kluczem dynamicznym określono grupę z kluczem dynamicznym i identyfikator zdalnego serwera kluczy. Później, po wybraniu opcji **Właściwości** powiązanego obiektu połączenia, na stronie **Ogółe** arkusza właściwości wyświetlany jest ten sam identyfikator zdalnego serwera kluczy, ale inna grupa z kluczem dynamicznym.

### Możliwe rozwiązanie:

Identyfikator to jedyna informacja przechowywana w bazie strategii VPN dotycząca zdalnego serwera kluczy dla połączenia z kluczem dynamicznym. Kiedy interfejs VPN szuka zdalnego serwera kluczy w strategii, najpierw wyszukuje grupę z kluczem dynamicznym, w której znajduje się identyfikator tego zdalnego serwera kluczy. Tym samym podczas wyświetlania właściwości dla takich połączeń, używana jest ta sama grupa z kluczem dynamicznym, którą znalazł interfejs VPN. Aby nie wiązać grupy z kluczem dynamicznym z tym zdalnym serwerem kluczy, można wykonać jedną z następujących czynności:

1. Usunąć zdalny serwer kluczy z grupy z kluczem dynamicznym.
2. Rozwinąć pozycję **Według grup** w lewej części okna interfejsu VPN i przeciągnąć odpowiednią grupę z kluczem dynamicznym na początek tabeli wyświetlanej w prawej części okna. Dzięki temu interfejs VPN będzie szukał zdalnego serwera kluczy najpierw w tej grupie z kluczem dynamicznym.

## Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QIPFILTER

Kronika QIPFILTER znajduje się w bibliotece QUSRSYS i zawiera informacje o zestawach reguł filtrowania oraz informacje, czy dany datagram IP został przepuszczony, czy zablokowany. Protokołowanie odbywa się zgodnie z opcjami kronikowania określonymi w regułach filtrowania.

### Włączenie kroniki IP Packet Filter (QIPFILTER)

Do uaktywnienia kroniki QIPFILTER służy Edytor reguł pakietów programu iSeries<sup>(TM)</sup> Navigator. Funkcje protokołowania trzeba włączyć dla każdej indywidualnej reguły filtrowania. Nie ma funkcji umożliwiającej protokołowanie dla wszystkich przychodzących lub wychodzących datagramów IP.

**Uwaga:** Włączenie kroniki QIPFILTER jest możliwe tylko po wcześniejszej dezaktywacji filtrów.

Aby włączyć kronikowanie dla konkretnej reguły filtrowania, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** i wybierz opcję **Konfigurowanie**. Spowoduje to wyświetlenie interfejsu Reguły pakietów.
3. Otwórz istniejący plik reguł filtrowania.
4. Dwukrotnie kliknij regułę filtrowania, dla której chcesz włączyć kronikowanie.
5. W polu **Kronikowanie** na stronie **Ogólne** wybierz wartość **FULL**, jak to pokazano w poniższym oknie dialogowym. Spowoduje to włączenie protokołowania dla danej reguły filtrowania.
6. Kliknij przycisk **OK**.
7. Zapisz zmieniony plik reguł filtrowania i uaktywnij go.

W kronice QIPFILTER będą zapisywane pozycje dla datagramów IP zgodnych z definicjami reguły filtrowania.

### Korzystanie z kroniki QIPFILTER

System OS/400<sup>(R)</sup> automatycznie tworzy kronikę podczas pierwszego uaktywnienia filtrowania pakietów IP. Aby wyświetlić szczegóły dla danej pozycji w kronice, można wyświetlić pozycje kroniki na ekranie lub użyć zbioru wyjściowego.

Kopiując pozycje z kroniki do zbioru wyjściowego, można je w łatwy sposób przeglądać za pomocą narzędzi do tworzenia zapytań, takich jak Query/400 lub SQL. Można także samodzielnie napisać programy w języku HLL, które będą przetwarzać pozycje w zbiorze wyjściowym.

Poniżej przedstawiono przykład zastosowania komendy Wyświetlenie kroniki (Display Journal - DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTYP((TF)) OUTPUT(*OUTFILE)
      OUTFILFMT(*TYPE4) OUTFILE(moja_biblioteka/moj_zbior) ENTDTALEN(*VARLEN *CALC)
```

Aby skopiować pozycje z kroniki QIPFILTER do zbioru wyjściowego, wykonaj następujące czynności:

1. Skopiuj dostarczany z systemem zbiór wyjściowy QSYS/QATOFIPF do biblioteki użytkownika, korzystając z komendy Tworzenie duplikatu obiektu (Create Duplicate Object - CRTDUPOBJ). Poniżej przedstawiono przykład zastosowania komendy CRTDUPOBJ:

```
CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(moja_biblioteka)
      NEWOBJ(moj_zbior)
```

2. Użyj komendy Wyświetlenie kroniki (Display Journal - DSPJRN) do skopiowania pozycji z kroniki QUSRSYS/QIPFILTER do zbioru wyjściowego utworzonego w poprzednim punkcie.

Jeśli zastosuje się komendę DSPJRN dla nieistniejącego zbioru wyjściowego, system utworzy taki zbiór, ale nie będzie on zawierał poprawnych opisów pól.

**Uwaga:** Kronika QIPFILTER zawiera pozycje dotyczące przepuszczania i blokowania tylko wtedy, gdy opcja kronikowania ma wartość FULL. Jeśli na przykład zostaną zdefiniowane wyłącznie reguły filtrowania typu PERMIT, datagramy IP, które nie są dopuszczone w sposób jawny, będą blokowane. Dla tych zablokowanych datagramów nie będą zapisywane pozycje w kronice. Na potrzeby analizy problemów można dodać regułę filtrowania, która w sposób jawny zablokuje cały pozostały ruch i będzie kronikowana z opcją FULL. Wówczas w kronice będą zapisywane pozycje typu DENY dla wszystkich datagramów IP, które zostały zablokowane. Ze względu na wydajność nie zaleca się włączania kronikowania dla wszystkich reguł filtrowania. Po przetestowaniu zestawów filtrów należy ograniczyć kronikowanie do przydatnego podzbioru pozycji.

W sekcji “Pola kroniki QIPFILTER” znajduje się tabela opisująca zbiór wyjściowy kroniki QIPFILTER.

## Pola kroniki QIPFILTER

W poniższej tabeli przedstawiono opisy pól zbioru wyjściowego QIPFILTER:

Nazwa pola	Długość pola	Liczbowe	Opis	Komentarze
TFENTL	5	T	Długość pozycji	
TFSEQN	10	T	Numer kolejny	
TFCODE	1	N	Kod kroniki	Zawsze M
TFENTT	2	N	Typ pozycji	Zawsze TF
TFTIME	26	N	Datownik SAA	
TFJOB	10	N	Nazwa zadania	
TFUSER	10	N	Profil użytkownika	
TFNBR	6	T	Numer zadania	
TFPGM	10	N	Nazwa programu	
TFRES1	51	N	Zastrzeżone	
TFUSPF	10	N	Użytkownik	
TFSYMN	8	N	Nazwa systemu	
TFRES2	20	N	Zastrzeżone	
TFRESA	50	N	Zastrzeżone	
TFLINE	10	N	Opis linii	*ALL jeśli TFREVT jest równe U*, puste jeśli TFREVT jest równe L*, Nazwa linii jeśli TFREVT jest równe L
TFREVT	2	N	Zdarzenie reguły	L* lub L, kiedy reguły są ładowane (load). U* gdy reguły są rozładowywane (unload), A dla działania filtru (action)
TFPDIR	1	N	Kierunek pakietu IP	O - wychodzące (outbound), I - przychodzące (inbound)
TFRNUM	5	N	Numer reguły	Dotyczy numeru reguły w aktywnym pliku reguł
TFACT	6	N	Działanie podjęte przez filtr	PERMIT, DENY lub IPSEC
TFPROT	4	N	Protokół transportowy	1 - protokół ICMP 6 - protokół TCP 17 - protokół UDP 50 - protokół ESP 51 - protokół AH
TFSRCA	15	N	Źródłowy adres IP	
TFSRCP	5	N	Port źródłowy	Czyszczenie jeśli TFPROT=1 (ICMP)
TFDSTA	15	N	Docelowy adres IP	
TFDSTP	5	N	Port docelowy	Czyszczenie jeśli TFPROT=1 (ICMP)

Nazwa pola	Długość pola	Liczbowe	Opis	Komentarze
TFTEXT	76	N	Dodatkowy tekst	Zawiera opis jeśli TFREVT=L* lub U*

## Rozwiązywanie problemów dotyczących połączeń VPN za pomocą kroniki QVPN

Do protokołowania informacji dotyczących ruchu IP i połączeń interfejs VPN używa osobnej kroniki o nazwie QVPN. Kronika QVPN jest przechowywana w bibliotece QUSRSYS. Kod kroniki wynosi M a typ kroniki to TS. Z pozycji tej kroniki rzadko korzysta się podczas codziennej pracy. Mogą one natomiast być przydatne podczas rozwiązywania problemów oraz weryfikowania prawidłowego działania systemu, kluczy i połączeń. Pozycje kroniki mogą na przykład pomóc zorientować się w przepływie pakietów danych. Informują one także o bieżącym statusie połączenia VPN.

### Włączenie kroniki QVPN

Kronikę VPN uaktywnia się za pomocą interfejsu wirtualnych sieci prywatnych w programie iSeries<sup>(TM)</sup> Navigator. Nie ma funkcji umożliwiającej protokołowanie wszystkich połączeń VPN. Dlatego funkcję protokołowania trzeba włączyć osobno dla każdej grupy z kluczem dynamicznym lub dla każdego połączenia ręcznego.

Aby włączyć kronikowanie dla konkretnej grupy z kluczem dynamicznym lub połączenia ręcznego, wykonaj następujące czynności:

1. W programie iSeries Navigator rozwiń pozycję serwer → **Sieć** → **Strategie IP** → **Sieć VPN** → **Połączenia chronione**.
2. Dla grupy z kluczem dynamicznym rozwiń pozycję **Według grupy**, a następnie kliknij prawym przyciskiem myszy grupę z kluczem dynamicznym, dla której chcesz włączyć kronikowanie, i wybierz opcję **Właściwości**.
3. Dla połączeń ręcznych rozwiń pozycję **Wszystkie połączenia**, a następnie kliknij prawym przyciskiem myszy połączenie ręczne, dla którego chcesz włączyć kronikowanie.
4. Na stronie **Ogólne** wybierz wymagany poziom kronikowania. Dostępne są cztery opcje. Są to:
  - Brak**  
Dla tej grupy połączeń kronikowanie będzie wyłączone.
  - Wszystko**  
Kronikowanie będzie obejmować wszystkie działania związane z połączeniem, takie jak uruchamianie i zatrzymywanie połączenia, odświeżanie kluczy, a także informacje o ruchu IP.
  - Działanie połączenia**  
Kronikowanie obejmie takie działania, jak uruchamianie i zatrzymywanie połączenia.
  - Ruch IP**  
Kronikowanie obejmie cały ruch VPN powiązany z tym połączeniem. Podczas każdego wywołania reguły filtrowania w protokole będą zapisywane pozycje. System rejestruje informacje dotyczące ruchu IP w kronice QIPFILTER, która znajduje się w bibliotece QUSRSYS.
5. Kliknij przycisk **OK**.
6. Uruchom połączenie, aby uaktywnić kronikowanie.

**Uwaga:** Zatrzymanie kronikowania jest możliwe tylko wtedy, gdy połączenie jest nieaktywne. Aby zmienić status kronikowania dla grupy połączeń, należy się upewnić, że żadne aktywne połączenie nie jest powiązane z tą grupą.

### Korzystanie z kroniki QVPN

Aby wyświetlić szczegóły dla danej pozycji w kronice QVPN, można wyświetlić pozycje kroniki na ekranie lub użyć zbioru wyjściowego.

Po skopiowaniu pozycji z kroniki do zbioru wyjściowego, można je w łatwy sposób przeglądać za pomocą narzędzi do tworzenia zapytań, takich jak Query/400 lub SQL. Można także samodzielnie napisać programy w języku HLL, które będą przetwarzać pozycje w zbiorze wyjściowym. Poniżej przedstawiono przykład zastosowania komendy Wyświetlenie kroniki (Display Journal - DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
  OUTFILE(moja_biblioteka/moj_zbior) ENTDTALEN(*VARLEN *CALC)
```

Aby skopiować pozycje z kroniki QVPN do zbioru wyjściowego, wykonaj następujące czynności:

1. Skopiuj dostarczany z systemem zbiór wyjściowy QSYS/QATOVSOFF do biblioteki użytkownika. Można to zrobić, korzystając z komendy Tworzenie duplikatu obiektu (Create Duplicate Object - CRTDUPOBJ). Poniżej przedstawiono przykład zastosowania komendy CRTDUPOBJ:

```
CRTDUPOBJ OBJ(QATOVSOFF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(moja_biblioteka)
  NEWOBJ(moj_zbior)
```

2. Użyj komendy Wyświetlenie kroniki (Display Journal - DSPJRN) w celu skopiowania pozycji z kroniki QUSRSYS/QVPN do zbioru wyjściowego utworzonego w poprzednim punkcie. Jeśli użyje się komendy DSPJRN dla nieistniejącego zbioru wyjściowego, system utworzy taki zbiór, ale nie będzie on zawierał poprawnych opisów pól.

W sekcji “Pola kroniki QVPN” znajduje się tabela opisująca zbiór wyjściowy kroniki QVPN.

## Pola kroniki QVPN

W poniższej tabeli przedstawiono opisy pól zbioru wyjściowego QVPN:

Nazwa pola	Długość pola	Liczbowe	Opis	Komentarze
TSENTL	5	T	Długość pozycji	
TSSEQN	10	T	Numer kolejny	
TSCODE	1	N	Kod kroniki	Zawsze M
TSENTT	2	N	Typ pozycji	Zawsze TS
TSTIME	26	N	Datownik pozycji SAA	
TSJOB	10	N	Nazwa zadania	
TSUSER	10	N	Użytkownik zadania	
TSNBR	6	T	Numer zadania	
TSPGM	10	N	Nazwa programu	
TSRES1	51	N	Nieużywane	
TSUSPF	10	N	Nazwa profilu użytkownika	
TSSYNM	8	N	Nazwa systemu	
TSRES2	20	N	Nieużywane	
TSRESA	50	N	Nieużywane	
TSESDL	4	T	Długość konkretnych danych	
TSCMPN	10	N	Komponent VPN	
TSCONM	40	N	Nazwa połączenia	
TSCOTY	10	N	Typ połączenia	
TSCOS	10	N	Stan połączenia	
TSCOSD	8	N	Data uruchomienia	
TSCOST	6	N	Godzina uruchomienia	
TSCOED	8	N	Data zakończenia	
TSCOET	6	N	Godzina zakończenia	
TSTRPR	10	N	Protokół transportowy	
TSLCAD	43	N	Adres lokalnego klienta	
TSLCPR	11	N	Porty lokalne	
TSRCAD	43	N	Adres zdalnego klienta	



Nazwa pola	Długość pola	Liczbowe	Opis	Komentarze
TSCPR	11	N	Porty zdalne	
TSLEP	43	N	Lokalny punkt końcowy	
TSREP	43	N	Zdalny punkt końcowy	
TSCORF	6	N	Liczba odświeżeń	
TSRFDA	8	N	Data następnego odświeżenia	
TSRFTI	6	N	Godzina następnego odświeżenia	
TSRFLS	8	N	Wielkość odświeżania	
TSSAPH	1	N	Faza SA	
TSAUTH	10	N	Typ uwierzytelniania	
TSENCR	10	N	Typ szyfrowania	
TSDHGR	2	N	Grupa Diffie-Hellman	
TSERRC	8	N	Kod błędu	

## Rozwiązywanie problemów dotyczących połączeń VPN za pomocą protokołów zadań VPN

W razie pojawienia się problemów dotyczących połączeń VPN zawsze zaleca się przeanalizowanie protokołów zadań. Jest kilka protokołów zadań, które zawierają komunikaty o błędach i dodatkowe informacje dotyczące środowiska VPN.

Jeśli po obu stronach połączenia są serwery iSeries<sup>(TM)</sup>, ważne jest przeanalizowanie protokołów zadań w obydwu tych systemach. Kiedy nie można uruchomić połączenia dynamicznego, dobrze jest wiedzieć, co się dzieje w zdalnym systemie.

Zadania VPN, QTOVMAN i QTOKVPNIKE działają w podsystemie QSYSWRK. Protokoły tych zadań można “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 za pomocą programu OS/400<sup>(R)</sup> iSeries Navigator.

W sekcji tej krótko opisano najważniejsze zadania środowiska VPN. Poniższa lista przedstawia nazwy zadań i krótkie objaśnienie ich przeznaczenia:

### QTCPIP

Jest to zadanie podstawowe, które uruchamia wszystkie interfejsy TCP/IP. W razie wystąpienia podstawowych problemów z protokołem TCP/IP należy zanalizować protokół zadania QTCPIP.

### QTOKVPNIKE

Zadanie QTOKVPNIKE to zadanie VPN Key Manager. VPN Key Manager nasłuchuje na porcie 500 protokołu UDP, aby przetwarzać protokół IKE (Internet Key Exchange).

### QTOVMAN

Jest to zadanie Menedżera połączeń VPN. Protokół tego zadania zawiera “Często spotykane komunikaty o błędach Menedżera połączeń VPN” na stronie 60 dla każdej nieudanej próby połączenia.

### QTPPANSxxx

Jest to zadanie używane dla połączeń modemowych PPP. Jeśli w profilu PPP zdefiniowany jest parametr \*ANS, zadanie to odpowiada na próby połączeń.

### QTPPPCTL

Jest to zadanie dla wychodzących połączeń modemowych PPP.

### QTPPPL2TP

Jest to zadanie menedżera protokołu L2TP (Layer Two Tunneling Protocol). Jeśli pojawią się problemy ze skonfigurowaniem tunelu L2TP należy przejrzeć komunikat w protokole tego zadania.

## Często spotykane komunikaty o błędach Menedżera połączeń VPN

W tej sekcji opisano niektóre z częściej występujących komunikatów o błędach Menedżera połączeń VPN.

Kiedy w połączeniu VPN wystąpi błąd, Menedżer połączeń VPN protokołuje dwa komunikaty w protokole zadania QTOVMAN. Pierwszy komunikat zawiera szczegóły dotyczące błędu. W programie iSeries<sup>(TM)</sup> Navigator informacje te można wyświetlić klikając prawym przyciskiem myszy połączenie, w którym wystąpił błąd i wybierając opcję **Informacje o błędzie**.

Drugi komunikat opisuje czynność, którą próbowano wykonać, kiedy wystąpił błąd. Na przykład uruchamianie lub zatrzymywanie połączenia. Typowymi przykładami komunikatów tego rodzaju są opisane poniżej komunikaty TCP8601, TCP8602 i TCP860A.

### Komunikaty o błędach Menedżera połączeń VPN

Komunikat	Przyczyna	Działanie
TCP8601 Nie można uruchomić połączenia VPN [nazwa połączenia]	Nie można uruchomić tego połączenia ze względu na jeden z poniższych kodów przyczyn: 0 - poprzedni komunikat z tą samą nazwą połączenia VPN zawiera bardziej szczegółowe informacje. 1 - konfiguracja strategii VPN. 2 - awaria sieci komunikacyjnej. 3 - VPN Key Manager nie mógł wynegocjować nowego Security Association. 4 - zdalny punkt końcowy tego połączenia jest nieprawidłowo skonfigurowany. 5 - VPN Key Manager nie odpowiedział na żądanie Menedżera połączeń VPN. 6 - awaria ładowania komponentu IP Security połączenia VPN. 7 - awaria komponentu PPP.	<ol style="list-style-type: none"><li>1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.</li><li>2. Usuń błędy i spróbuj ponowić żądanie.</li><li>3. Użyj programu iSeries Navigator do “Wyświetlanie atrybutów połączeń aktywnych” na stronie 46. Połączenia, których nie udało się uruchomić, będą w stanie błędu.</li></ol>
TCP8602 Wystąpił błąd podczas zatrzymywania połączenia VPN [nazwa połączenia]	Zażądano zatrzymania wymienionego połączenia VPN, jednak nie zatrzymało się ono lub zatrzymało z błędem o kodzie przyczyny: 0 - poprzedni komunikat z tą samą nazwą połączenia VPN zawiera bardziej szczegółowe informacje. 1 - połączenie VPN nie istnieje. 2 - awaria wewnętrznej komunikacji z VPN Key Manager. 3 - awaria wewnętrznej komunikacji z komponentem IPSec. 4 - awaria komunikacji ze zdalnym punktem końcowym połączenia VPN.	<ol style="list-style-type: none"><li>1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.</li><li>2. Usuń błędy i spróbuj ponowić żądanie.</li><li>3. Użyj programu iSeries Navigator do “Wyświetlanie atrybutów połączeń aktywnych” na stronie 46. Połączenia, których nie udało się uruchomić, będą w stanie błędu.</li></ol>

## Komunikat

TCP8604

Uruchomienie połączenia VPN [*nazwa połączenia*] nie powiodło się

## Przyczyna

Uruchomienie tego połączenia nie powiodło się ze względu na jeden z poniższych kodów przyczyn:

- 1 - nie można przetłumaczyć nazwy zdalnego hosta na adres IP.
- 2 - nie można przetłumaczyć nazwy lokalnego hosta na adres IP.
- 3 - nie załadowano reguły filtrowania strategii VPN powiązanej z tym połączeniem VPN.
- 4 - podana przez użytkownika wartość klucza jest niepoprawna dla powiązanego algorytmu.
- 5 - wartość inicjująca dla połączenia VPN nie zezwala na daną czynność.
- 6 - rola systemu w połączeniu VPN jest niezgodna z informacjami z grupy połączeń.
- 7 - zastrzeżone.
- 8 - punkty końcowe danych (lokalne i zdalne adresy i usługi) tego połączenia VPN są niezgodne z informacjami z grupy połączeń.
- 9 - niepoprawny typ identyfikatora.

## Działanie

1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.
2. Usuń błędy i spróbuj ponowić żądanie.
3. Użyj programu iSeries Navigator do sprawdzenia lub poprawienia konfiguracji strategii VPN. Sprawdź, czy w grupie z kluczem dynamicznym powiązanej z tym połączeniem skonfigurowano dopuszczalne wartości.

TCP8605

Menedżer połączeń VPN nie mógł nawiązać komunikacji z VPN Key Manager

Menedżer połączeń VPN wymaga usług VPN Key Manager do ustanowienia powiązania Security Association dla dynamicznych połączeń VPN. Menedżer połączeń VPN nie mógł nawiązać komunikacji z VPN Key Manager.

1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.
2. Sprawdź, czy interfejs \*LOOPBACK jest aktywny, używając komendy NETSTAT OPTION(\*IFC).
3. Zakończ działanie serwera VPN, używając komendy ENDTCPSVR SERVER(\*VPN). Następnie restartuj serwer VPN za pomocą komendy STRTCPSRV SERVER(\*VPN).  
**Uwaga:** Spowoduje to zakończenie wszystkich bieżących połączeń.

## Komunikat

TCP8606

VPN Key Manager nie mógł ustanowić żądanego powiązania Security Association dla połączenia [*nazwa połączenia*]

## Przyczyna

VPN Key Manager nie mógł ustanowić żądanego powiązania Security Association ze względu na jeden z poniższych kodów przyczyn:

24 - uwierzytelnienie połączenia klucza VPN Key Manager nie powiodło się.  
8300 - awaria podczas negocjacji połączenia klucza VPN Key Manager.  
8306 - nie znaleziono lokalnego wstępnego klucza współużytkowanego.  
8307 - nie znaleziono zdalnej strategii fazy 1. IKE.  
8308 - nie znaleziono zdalnego wstępnego klucza współużytkowanego.  
8327 - upłynął limit czasu negocjacji połączenia klucza VPN Key Manager.  
8400 - awaria podczas negocjacji połączenia VPN Key Manager.  
8407 - nie znaleziono zdalnej strategii fazy 2. IKE.  
8408 - upłynął limit czasu negocjacji połączenia VPN Key Manager.  
8500 lub 8509 - wystąpił błąd w sieci VPN Key Manager.

## Działanie

1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.
2. Usuń błędy i spróbuj ponowić żądanie.
3. Użyj programu iSeries Navigator do sprawdzenia lub poprawienia konfiguracji strategii VPN. Sprawdź, czy w grupie z kluczem dynamicznym powiązanej z tym połączeniem skonfigurowano dopuszczalne wartości.

TCP8608

Połączenie VPN [*nazwa połączenia*] nie mogło uzyskać adresu NAT

Dla grupy z kluczem dynamicznym lub połączenia danych określono translację NAT na jeden lub kilka adresów. Translacja ta nie powiodła się z uwagi na jeden z następujących kodów przyczyn:  
1 - adres, który ma być poddany translacji NAT, nie jest pojedynczym adresem.  
2 - wszystkie dostępne adresy zostały użyte.

1. Sprawdź dodatkowe komunikaty o błędach w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46.
2. Usuń błędy i spróbuj ponowić żądanie.
3. Użyj programu iSeries Navigator do sprawdzenia lub poprawienia strategii VPN. Sprawdź, czy w grupie z kluczem dynamicznym powiązanej z tym połączeniem skonfigurowano dopuszczalne wartości dla adresów.

TCP8620

Lokalny punkt końcowy połączenia jest niedostępny

Nie można włączyć tego połączenia VPN, ponieważ lokalny punkt końcowy połączenia jest niedostępny.

1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.
2. Sprawdź, czy lokalny punkt końcowy połączenia został zdefiniowany i uruchomiony, używając komendy NETSTAT OPTION(\*IFC).
3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

## Komunikat

TCP8621

Lokalny punkt końcowy danych jest niedostępny

## Przyczyna

Nie można włączyć tego połączenia VPN, ponieważ lokalny punkt końcowy danych jest niedostępny.

## Działanie

1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.
2. Sprawdź, czy lokalny punkt końcowy połączenia został zdefiniowany i uruchomiony, używając komendy NETSTAT OPTION(\*IFC).
3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

TCP8622

Brama nie zezwala na hermetyzację transportową

Nie można włączyć tego połączenia VPN, ponieważ wynegocjowana strategia określa tryb hermetyzacji transportowej, a to połączenie jest zdefiniowane jako brama ochrony.

1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.
2. Użyj programu iSeries Navigator do zmiany strategii VPN powiązanej z tym połączeniem VPN.
3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

TCP8623

Połączenie VPN nakłada się na połączenie istniejące

Nie można włączyć tego połączenia VPN, ponieważ jest już włączone istniejące połączenie VPN. Połączenie to ma lokalny punkt końcowy danych o wartości [wartość lokalnego punktu końcowego danych] i zdalny punkt końcowy danych o wartości [wartość zdalnego punktu końcowego danych].

1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.
2. W programie iSeries Navigator wyświetl wszystkie włączone połączenia, których lokalne i zdalne punkty końcowe danych pokrywają się z danym połączeniem. Jeśli potrzebne są obydwie połączenia, zmień strategię połączenia istniejącego.
3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

TCP8624

Połączenie VPN poza zasięgiem powiązanej reguły filtrowania strategii

Nie można włączyć tego połączenia VPN, ponieważ punkty końcowe danych znajdują się poza zdefiniowaną regułą filtrowania strategii.

1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.
2. W programie iSeries Navigator wyświetl ograniczenia punktu końcowego danych dla danego połączenia lub grupy z kluczem dynamicznym. Jeśli wybrane są opcje **Podzbiór filtru strategii** lub **Dostosuj do filtru strategii**, sprawdź punkty końcowe danych dla połączenia. Muszą one być zgodne z aktywną regułą filtrowania o akcji IPSEC, powiązaną z nazwą tego połączenia VPN. Zmień istniejącą strategię dla połączenia lub regułę filtrowania, aby włączyć to połączenie.
3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

Komunikat	Przyczyna	Działanie
TCP8625 Sprawdzanie algorytmu ESP przez połączenie VPN nie powiodło się	Nie można włączyć tego połączenia VPN, ponieważ klucz tajny powiązany z połączeniem jest niewystarczający.	<ol style="list-style-type: none"> <li>1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.</li> <li>2. W programie iSeries Navigator wyświetl strategię powiązaną z tym połączeniem i wpisz inny klucz tajny.</li> <li>3. Usuń wszelkie błędy i spróbuj ponowić żądanie.</li> </ol>
TCP8626 Punkt końcowy połączenia VPN jest inny niż punkt końcowy danych	Nie można włączyć tego połączenia VPN ponieważ według strategii jest to połączenie hosta, a punkt końcowy połączenia VPN jest inny niż punkt końcowy danych.	<ol style="list-style-type: none"> <li>1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.</li> <li>2. W programie iSeries Navigator wyświetl ograniczenia punktu końcowego danych dla danego połączenia lub grupy z kluczem dynamicznym. Jeśli wybrane są opcje <b>Podzbiór filtru strategii</b> lub <b>Dostosuj do filtru strategii</b>, sprawdź punkty końcowe danych dla połączenia. Muszą one być zgodne z aktywną regułą filtrowania o akcji IPSEC, powiązaną z nazwą tego połączenia VPN. Zmień istniejącą strategię dla połączenia lub regułę filtrowania, aby włączyć to połączenie.</li> <li>3. Usuń wszelkie błędy i spróbuj ponowić żądanie.</li> </ol>
TCP8628 Nie załadowano reguły filtrowania połączenia	Reguła filtrowania strategii dla tego połączenia jest nieaktywna.	<ol style="list-style-type: none"> <li>1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.</li> <li>2. W programie iSeries Navigator wyświetl aktywne filtry strategii. Sprawdź regułę filtrowania strategii dla tego połączenia.</li> <li>3. Usuń wszelkie błędy i spróbuj ponowić żądanie.</li> </ol>
TCP8629 Usunięto pakiet IP dla połączenia VPN	Dla tego połączenia VPN skonfigurowano translację VPN NAT i wymagany zestaw adresów NAT przekroczył zestaw dostępnych adresów NAT.	<ol style="list-style-type: none"> <li>1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.</li> <li>2. W programie iSeries Navigator zwiększ liczbę adresów NAT przypisanych do tego połączenia VPN.</li> <li>3. Usuń wszelkie błędy i spróbuj ponowić żądanie.</li> </ol>



<b>Komunikat</b>	<b>Przyczyna</b>	<b>Działanie</b>
TCP862A Uruchomienie połączenia PPP nie powiodło się	To połączenie VPN zostało powiązane z profilem PPP. Po uruchomieniu połączenia próbowano uruchomić profil PPP, ale to się nie powiodło.	<ol style="list-style-type: none"> <li>1. Sprawdź w “Wyświetlanie protokołów zadań serwera VPN” na stronie 46 dodatkowe komunikaty dotyczące tego połączenia.</li> <li>2. Sprawdź protokół zadania powiązany z połączeniem PPP.</li> <li>3. Usuń wszelkie błędy i spróbuj ponowić żądanie.</li> </ol>

## Rozwiązywanie problemów dotyczących połączeń VPN za pomocą śledzenia komunikacji w systemie OS/400

System operacyjny OS/400<sup>(R)</sup> serwera iSeries<sup>(TM)</sup> umożliwia śledzenie danych w linii komunikacyjnej, takiej jak interfejs sieci lokalnej (LAN) lub sieci rozległej (WAN). Przeciętny użytkownik może nie rozumieć całej treści danych śledzenia. Można jednak wykorzystać pozycje śledzenia do określenia, czy zachodzi wymiana danych pomiędzy serwerem lokalnym a zdalnym.

### Uruchamianie śledzenia komunikacji

Komenda Uruchomienie śledzenia komunikacji (Start Communications Trace - STRCMNTRC) służy do uruchomienia śledzenia komunikacji w lokalnym systemie. Poniżej przedstawiono przykład zastosowania komendy STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('Problemy z VPN')
```

Parametry komendy objaśniono poniżej:

#### **CFGOBJ** (Obiekt konfiguracyjny)

Nazwa obiektu konfiguracyjnego, który ma być śledzony. Obiektem jest opis linii, opis interfejsu sieciowego albo opis serwera sieciowego.

#### **CFGTYPE** (Typ konfiguracji)

Określa, czy śledzona jest linia (\*LIN), interfejs sieciowy (\*NWI), czy serwer sieciowy (\*NWS).

#### **MAXSTG** (Wielkość buforu)

Wielkość buforu na potrzeby śledzenia. Wartość domyślna wynosi 128 kB. Zakres wartości wynosi od 128 kB do 64 MB. Rzeczywista maksymalna wielkość buforu systemowego jest definiowana w narzędziach SST (System Service Tools). Dlatego podczas próby wykorzystania dla komendy STRCMNTRC buforu większego niż zdefiniowany w narzędziach SST, może zostać wygenerowany komunikat o błędzie. Należy pamiętać, że suma wielkości wszystkich buforów określonych dla wszystkich uruchomionych operacji śledzenia komunikacji nie może przekraczać maksymalnej wielkości buforu zdefiniowanej w narzędziach SST.

#### **DTADIR** (Kierunek danych)

Kierunek ruchu danych, które mają być śledzone. Parametr może określać tylko ruch wychodzący (\*SND), tylko ruch przychodzący (\*RCV) lub ruch w obydwu kierunkach (\*BOTH).

#### **TRCFULL** (Pełny bufor śledzenia)

Określa sposób postępowania, kiedy bufor jest pełny. Parametr ten ma dwie możliwe wartości. Wartość domyślna to \*WRAP, przy której po wypełnieniu buforu dane są zapisywane od początku. Najstarsze rekordy śledzenia są nadpisywane przez rekordy nowsze w miarę ich gromadzenia.

Druga wartość, \*STOPTRC, umożliwia zatrzymanie śledzenia, kiedy bufor śledzenia określony parametrem MAXSTG jest pełny. Zawsze należy definiować wielkość buforu na tyle dużą, aby pomieścił on wszystkie rekordy śledzenia. Zawijanie zapisu może spowodować utratę ważnych informacji o śledzeniu. W razie problemu występującego sporadycznie, należy zdefiniować bufor na tyle duży, aby zawijanie zapisu nie powodowało skasowania żadnych ważnych informacji.

### **USRDTA** (Liczba bajtów użytkownika do śledzenia)

Definiuje liczbę danych do śledzenia w części danych użytkownika ramek danych. Dla interfejsów LAN domyślnie przechwytywanych jest tylko pierwszych 100 bajtów danych użytkownika. Dla pozostałych interfejsów przechwytywane są wszystkie dane użytkownika. Jeśli przewiduje się problemy dotyczące części ramki z danymi użytkownika, należy określić wartość \*MAX.

### **TEXT** (Opis śledzenia)

Czytelny opis śledzenia.

## **Zatrzymywanie śledzenia komunikacji**

Śledzenie zazwyczaj jest zatrzymywane bezpośrednio po wystąpieniu warunku, którego śledzenie dotyczy, chyba że użytkownik określi inaczej. Do zatrzymywania śledzenia służy komenda Zakończenie śledzenia komunikacji (End Communications Trace - ENDCMNTRC). Poniżej przedstawiono przykład zastosowania komendy ENDCMNTRC:

```
ENDCMNTRC CFGOBJ(TRNLIN) CFGTYPE(*LIN)
```

Komenda ma dwa parametry:

### **CFGOBJ** (Obiekt konfiguracyjny)

Nazwa obiektu konfiguracyjnego, dla którego uruchamiane jest śledzenie. Obiektem jest opis linii, opis interfejsu sieciowego albo opis serwera sieciowego.

### **CFGTYPE** (Typ konfiguracji)

Określa, czy śledzona jest linia (\*LIN), interfejs sieciowy (\*NWI), czy serwer sieciowy (\*NWS).

## **Drukowanie danych śledzenia**

Po zatrzymaniu śledzenia komunikacji należy wydrukować dane śledzenia. Do wykonania tego zadania służy komenda Drukowanie śledzenia komunikacji (Print Communications Trace - PRTCMNTRC). Ponieważ w okresie śledzenia przechwytywany jest cały ruch linii, do wygenerowania danych wyjściowych dostępnych jest wiele opcji filtrowania. Należy starać się, aby zbiór buforowy był jak najmniejszy. Przyspieszy to analizę i poprawi jej efektywność. W wypadku problemu z połączeniem VPN należy filtrować tylko ruch IP i tylko dla określonego adresu (jeśli to możliwe). Możliwe jest także filtrowanie dla określonego numeru portu IP. Poniżej przedstawiono przykład zastosowania komendy PRTCMNTRC:

```
PRTCMNTRC CFGOBJ(TRNLIN) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)  
SLTPORT(500) FMTBCD(*NO)
```

W tym przykładzie śledzenie dotyczy tylko ruchu IP i obejmuje tylko te dane, dla których źródłowy lub docelowy adres IP wynosi 10.50.21.1, a numer źródłowego i docelowego portu IP wynosi 500.

Poniżej objaśniono tylko najważniejsze z punktu widzenia analizy problemów z połączeniami VPN parametry komend:

### **CFGOBJ** (Obiekt konfiguracyjny)

Nazwa obiektu konfiguracyjnego, dla którego uruchamiane jest śledzenie. Obiektem jest opis linii, opis interfejsu sieciowego albo opis serwera sieciowego.

### **CFGTYPE** (Typ konfiguracji)

Określa, czy śledzona jest linia (\*LIN), interfejs sieciowy (\*NWI), czy serwer sieciowy (\*NWS).

### **FMTTCP** (Formatowanie danych TCP/IP)

Określa, czy śledzenie ma być formatowane dla danych TCP/IP i UDP/IP. Należy użyć wartości \*YES, aby sformatować śledzenie danych IP.

### **TCPIPADR** (Formatowanie danych TCP/IP według adresów)

Parametr ten składa się z dwóch elementów. Jeśli zostaną określone adresy IP dla obydwu elementów, zostanie wydrukowany tylko ruch IP pomiędzy tymi adresami.

**SLTPORT** (Numer portu IP)  
Numer portu IP do filtrowania.

**FMTBCD** (Formatowanie danych rozgłaszania)  
Określa, czy mają być drukowane wszystkie ramki rozgłaszania. Wartość domyślna to \*YES. Aby na przykład nie drukować żądań protokołu ARP (Address Resolution Protocol), należy użyć wartości \*NO; w przeciwnym razie na wydruku będą dominować komunikaty rozgłaszania.

---

## Informacje pokrewne dla sieci VPN

Więcej scenariuszy i opisów konfiguracji sieci VPN można znaleźć w innych źródłach informacji:

- **OS/400<sup>(R)</sup> V5R1 Virtual Private Networks: Remote Access to the IBM<sup>(R)</sup> e(logo)server iSeries<sup>(TM)</sup> Server with Windows<sup>(R)</sup> 2000 VPN Clients, REDP0153**



W tej dokumentacji technicznej firmy IBM przedstawiono, krok po kroku, proces konfigurowania tunelu komunikacyjnego VPN za pomocą modułu V5R1 VPN oraz zintegrowanej z systemem Windows 2000 obsługi protokołów L2TP i IPSec.

- **AS/400<sup>(R)</sup> Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**



W tej dokumentacji technicznej przedstawiono koncepcje dotyczące sieci VPN oraz opisano ich implementację za pomocą protokołów IPSec i L2TP (Layer 2 Tunneling Protocol) w systemie OS/400.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**



W dokumencie tym opisano wszystkie zintegrowane opcje zabezpieczające dostępne w systemie OS/400, takie jak filtry IP, translację NAT, sieci VPN, serwer proxy HTTP, protokół SSL, usługi DNS, przekazywanie poczty, kontrole i protokołowanie. Praktyczne wykorzystanie tych opcji przedstawiono w nim w formie przystępnych przykładów.

- **Virtual Private Networking: Securing Connections**




Na tej stronie WWW przedstawiono nowości dotyczące sieci VPN, listę najnowszych poprawek PTF i odsyłacze do innych interesujących serwisów.

- **Inne podręczniki i dokumenty techniczne dotyczące ochrony**

Odsyłacz ten prowadzi do listy źródeł informacji dotyczących ochrony dostępnych online.

Aby zapisać plik PDF na stacji roboczej w celu wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Prawym przyciskiem myszy kliknij plik PDF w oknie przeglądarki (kliknij prawym przyciskiem myszy powyższy odsyłacz).
2. Kliknij opcję **Zapisz jako...**
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij przycisk **Zapisz**.

Kopię programu Adobe Acrobat Reader niezbędnego do wyświetlania i drukowania programu PDF można pobrać z serwisu internetowego firmy Adobe ([www.adobe.com/prodindex/acrobat/readstep.html](http://www.adobe.com/prodindex/acrobat/readstep.html)) .



---

## Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przysyłać na adres:

IBM Director of  
Licensing  
IBM Corporation  
500 Columbus Avenue  
Thornwood, NY 10594-1785  
U.S.A.

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japan

**Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:**INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ ("AS IS"), BEZ JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjodawcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation  
Software Interoperability Coordinator, Department 49XA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy są fikcyjne i jakiegokolwiek ich podobieństwo do nazwisk, nazw i adresów używanych w rzeczywistych przedsiębiorstwach jest całkowicie przypadkowe.

---

## Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

Application System/400  
AS/400  
e (logo)  
IBM  
iSeries  
Operating System/400  
OS/400  
400

Lotus, Freelance i WordPro są znakami towarowymi International Business Machines Corporation i Lotus Development Corporation w Stanach Zjednoczonych i/lub w innych krajach.

C-bus jest znakiem towarowym Corollary, Inc. w Stanach Zjednoczonych i/lub w innych krajach.



ActionMedia, LANDesk, MMX, Pentium oraz ProShare są znakami towarowymi lub zastrzeżonymi znakami towarowymi Intel Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT i logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

SET oraz logo SET są znakami towarowymi pozostającymi w posiadaniu SET Secure Electronic Transaction LLC.

Java oraz wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych firm, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

---

## Warunki pobierania i drukowania publikacji

Zezwolenie na korzystanie z publikacji, które Użytkownik zamierza pobrać, jest przyznawane na poniższych warunkach. Warunki te wymagają akceptacji Użytkownika.

**Użytek osobisty:** Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać z nich prac pochodnych bez wyraźnej zgody IBM.

**Użytek służbowy:** Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać z tych publikacji ani z ich części prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych. IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ ("AS-IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ CZY PRZYDATNOŚCI DO OKREŚLONEGO CELU.

Wszelkie materiały są chronione prawem autorskim IBM Corporation.

Pobieranie lub drukowanie publikacji z tego serwisu oznacza zgodę na warunki zawarte w niniejszym dokumencie.





**IBM**