System i

Bezpieczeństwo
Sieć VPN

Wersja 6 wydanie 1

System i

Bezpieczeństwo
Sieć VPN

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z niniejszych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w dodatku “Uwagi”, na stronie 81.

To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Sieć VPN (Virtual Private Network)

Sieć VPN umożliwia przedsiębiorstwu bezpieczne rozszerzenie prywatnego intranetu na istniejącą strukturę sieci publicznej, takiej jak Internet. Dzięki VPN firma może sterować ruchem w sieci przy jednoczesnym zapewnieniu ważnych opcji zabezpieczających, takich jak uwierzytelnianie i ochrona danych.

VPN to instalowany opcjonalnie komponent programu System i Navigator, graficznego interfejsu użytkownika systemu i5/OS. Pozwala on tworzyć zabezpieczone na całej długości ścieżki połączeń pomiędzy dowolnymi hostami i bramami. Sieć 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 V6R1

Poniżej omówiono nowe lub znacznie zmienione informacje w kolekcji tematów dotyczących sieci VPN.

Nowa funkcja: protokół IP wersja 6

Do tworzenia sieci VPN z połączeniami typu host-host, host-brama i brama-brama można teraz stosować protokół IP wersja 6. Połączenia VPN obsługują protokół IP wersja 6 w adresach, zakresach, podsieciach i nazwach hostów. Zaktualizowano wszystkie kreatory sieci VPN, aby akceptowały nowe typy identyfikatorów protokołu IP w wersji 6.

- Protokół IP wersja 6

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić odnalezienie miejsc, w których wprowadzono zmiany techniczne, użyto następujących symboli:

- symbol » służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol « służący do zaznaczania końca nowego lub zmienionego fragmentu.

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

Plik PDF z informacjami na temat sieci VPN

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

Aby wyświetlić lub pobrać ten dokument w formacie PDF, kliknij odsyłacz Sieć VPN (Virtual Private Network) (około 1100 kB).

Zapisywanie plików PDF

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

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij przycisk **Zapisz element docelowy jako**, jeśli używasz przeglądarki Internet Explorer. Kliknij przycisk **Zapisz łącze jako**, jeśli używasz przeglądarki Netscape Communicator.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Acrobat Reader

Do wyświetlania i drukowania plików PDF potrzebny jest program Adobe Acrobat Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Pojęcia związane z siecią VPN

Ważne jest, aby przed rozpoczęciem implementowania połączenia VPN mieć przynajmniej podstawową wiedzę o standardowych technologiach VPN.

Do zabezpieczenia przesyłanych danych w technologii wirtualnych sieci prywatnych (VPN) wykorzystuje się kilka ważnych protokołów TCP/IP. Aby lepiej zrozumieć sposób działania dowolnego połączenia VPN, należy poznać te protokoły oraz sposób ich wykorzystania przez sieć VPN:

Protokoły bezpieczeństwa IP

Protokół bezpieczeństwa IP (IP Security - IPSec) zapewnia stabilną, trwałą podstawę bezpieczeństwa w warstwie sieciowej.

Protokół IPSec obsługuje wszystkie używane współcześnie algorytmy szyfrujące i może także dostosować się do nowszych, silniejszych algorytmów, które pojawią 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 powiązaniami 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.

Uwaga: Niektóre konfiguracje połączenia VPN mogą mieć słabe punkty zabezpieczeń w zależności od konfiguracji protokołu IPSec. Te słabe punkty mają wpływ na konfiguracje, w których IPSec korzysta z protokołu ESP w

trybie tunelowym z użyciem szyfrowania, ale bez zabezpieczenia integralności (uwierzytelnianie) i bez nagłówka uwierzytelnienia (AH). Domyślna konfiguracja, gdy wybrany jest protokół ESP, zawsze zawiera algorytm uwierzytelnienia, który zapewnia zabezpieczenie integralności. Dlatego o ile algorytm uwierzytelnienia w transformacji ESP nie zostanie usunięty, konfiguracje VPN będą chronione przed tym słabym punktem zabezpieczeń. Konfiguracja IBM Universal Connection VPN nie jest narażona na ten słaby punkt zabezpieczeń.

Aby sprawdzić, czy słaby punkt zabezpieczeń ma wpływ na system, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Strategie bezpieczeństwa IP → Strategie danych**.
2. Kliknij prawym przyciskiem myszy strategię danych, którą chcesz sprawdzić, i wybierz opcję **Właściwości**.
3. Kliknij zakładkę **Propozycje**.
4. Wybierz dowolną z propozycji ochrony danych korzystającą z protokołu ESP i kliknij opcję **Edycja**.
5. Kliknij zakładkę **Transformacje**.
6. Wybierz z listy dowolną transformację korzystającą z protokołu ESP i kliknij opcję **Edycja**.
7. Sprawdź, czy algorytm uwierzytelnienia ma wartość inną niż **Brak**.

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 WWW pod adresem http://www.rfc-editor.org.

Główne protokoły IPSec opisano w kolejnych sekcjach.

Pojęcia pokrewne

"Zarządzanie kluczami" na stronie 6
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.

Informacje pokrewne

http://www.rfc-editor.org

Protokół AH (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 klucza współużytkowanego w swoim algorytmie uwierzytelniania. Do ochrony odpowiedzi protokół AH używa pola z numerem kolejnym w nagłówku AH. Warto tutaj zauważyć, że te trzy różne funkcje są często łączone i określane jako uwierzytelnianie. Mówiąc najprościej, AH gwarantuje, że nie manipulowano danymi w drodze do ich miejsca przeznaczenia.

Mimo że protokół AH uwierzytelnia maksymalną możliwą część datagramu IP, odbiorca nie może przewidzieć wartości niektórych pól z nagłówka IP. AH nie chroni tych pól, zwanych polami zmiennymi. Protokół ten zawsze jednak chroni dane ładunku 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 WWW pod adresem 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 ładunku 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 na dwóch bramach bezpieczeństwa może działać tunel AH służący do uwierzytelniania całego ruchu między połączonymi sieciami. 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 Encapsulating Security Payload (ESP) również może uwierzytelniać dane, jego zastosowanie znacznie wyraźniej odbija się na wydajności systemu niż 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.

Używanie numeru ESN razem z protokołem AH

Jeśli wykorzystywany jest protokół AH, to może okazać się konieczne aktywowanie numeru ESN. Umożliwia on przesyłanie dużych woluminów danych przy dużej szybkości bez ponownego szyfrowania za pomocą klucza. Połączenie VPN korzysta z 64-bitowych numerów kolejnych zamiast 32-bitowych numerów w IPSec. Używanie 64-bitowych numerów kolejnych wydłuża czas do wymiany klucza, co przeciwdziała wyczerpaniu numerów kolejnych i minimalizuje użycie zasobów systemowych.

Jakich algorytmów używa protokół AH do ochrony informacji?

Protokół AH wykorzystuje algorytmy zwane kodami **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 WWW pod adresem http://www.rfc-editor.org.

Pojęcia pokrewne

“Protokół ESP (Encapsulating Security Payload)”
Protokół Encapsulating Security Payload (ESP) zapewnia poufność danych, a opcjonalnie również uwierzytelnianie pochodzenia danych, sprawdzanie integralności i ochronę odpowiedzi.

Informacje pokrewne

http://www.rfc-editor.org

Protokół ESP (Encapsulating Security Payload)

Protokół Encapsulating Security Payload (ESP) zapewnia poufność danych, a opcjonalnie również uwierzytelnianie pochodzenia danych, sprawdzanie integralności i ochronę odpowiedzi.

Te same funkcje realizuje protokół Authentication Header (AH), 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.

Jakich algorytmów używa 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. Sieć VPN wykorzystuje następujące algorytmy szyfrowania: Data Encryption Standard (DES), triple-DES (3DES), RC5, RC4 lub Advanced Encryption Standard (AES).

Jeśli wybrano algorytm AES, możliwe, że wybrane będzie też włączenie numeru ESN. ESN umożliwia przesyłanie dużych woluminów danych przy dużej szybkości. Połączenie VPN korzysta z 64-bitowych numerów kolejnych zamiast 32-bitowych numerów w IPSec. Używanie 64-bitowych numerów kolejnych wydłuża czas do wymiany klucza, co przeciwdziała wyczerpaniu numerów kolejnych i minimalizuje użycie zasobów systemowych.

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*. Grupa wykonawcza IETF formalnie zdefiniowała algorytm 3DES w dokumencie 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.

Grupa wykonawcza IETF formalnie zdefiniowała algorytm HMAC-MD5 w dokumencie RFC 2085 zatytułowanym*HMAC-MD5 IP Authentication with Replay Prevention*. Grupa wykonawcza IETF formalnie zdefiniowała algorytm HMAC-SHA w dokumencie 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

Pojęcia pokrewne

“Protokół AH (Authentication Header)” na stronie 3
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.

Informacje pokrewne

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 pełne zabezpieczenie całego datagramu IP. Mimo iż połączenie obu protokołów poprawia bezpieczeństwo, związany z tym nakład pracy może być większy niż korzyści.

Zarządzanie kluczami

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.

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.

Menedżer kluczy VPN to opracowana przez firmę IBM 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 obydwa 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. Należy skonfigurować certyfikaty cyfrowe za pomocą menedżera certyfikatów cyfrowych. Ponadto podpis RSA jest wymagany do współdziałania niektórych rozwiązań dla sieci VPN. Na przykład, implementacja sieci VPN w systemie Windows 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 obydwa 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 obydwa 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 za pomocą programu System i Navigator konieczne jest zdefiniowanie strategii IKE, aby umożliwić fazę 1. negocjacji oraz zdefiniowanie strategii danych, 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 WWW pod adresem http://www.rfc-editor.org.

Pojęcia pokrewne

“Scenariusz: sieć VPN współpracująca z zaporami firewall” na stronie 29
W tym scenariuszu duża firma ubezpieczeniowa chce nawiązać połączenie VPN pomiędzy bramą w Poznaniu a hostem w Szczecinie, gdy obydwie sieci znajdują się za zaporami firewall.

“Protokoły bezpieczeństwa IP” na stronie 2
Protokół bezpieczeństwa IP (IP Security - IPSec) zapewnia stabilną, trwałą podstawę bezpieczeństwa w warstwie sieciowej.

Zadania pokrewne

“Konfigurowanie strategii protokołu IKE” na stronie 49
Strategia protokołu IKE (Internet Key Exchange) definiuje poziom ochrony uwierzytelniania i szyfrowania używany przez protokół IKE podczas negocjacji w fazie 1.

“Konfigurowanie strategii danych” na stronie 50
Strategia danych określa za pomocą uwierzytelniania i szyfrowania poziom ochrony, jaki zostanie użyty podczas przesyłania danych połączeniem VPN.

Informacje pokrewne

http://www.rfc-editor.org

Protokół L2TP (Layer 2 Tunneling Protocol)

Połączenia korzystające z protokołu L2TP (Layer 2 Tunneling Protocol), zwane również liniami wirtualnymi, zapewniają zdalnym użytkownikom ekonomiczną metodę dostępu poprzez umożliwienie systemom sieci korporacyjnych zarządzania adresami IP przypisanymi do tych użytkowników. 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 klienta zdalnego, a tunel przymusowy -- u dostawcy usług internetowych (ISP).

W przypadku **przymusowego tunelu** L2TP zdalny host inicjuje połączenie z dostawcą ISP. 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 dotyczącym zabezpieczania dobrowolnego tunelu L2TP za pomocą protokołu IPSec przedstawiono przykład konfigurowania systemu w biurze oddziału do połączeń z siecią przedsiębiorstwa poprzez system bram z tunelem L2TP zabezpieczonym mechanizmami sieci VPN.

Dostępna jest prezentacja wizualna przedstawiająca pojęcie dobrowolnych tuneli L2TP zabezpieczanych protokołem IPSec. Wymaga ona zainstalowania wtyczki Flash. Dostępna jest również wersja 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).

Pojęcia pokrewne

“Scenariusz: zabezpieczanie dobrowolnego tunelu L2TP za pomocą protokołu IPSec” na stronie 23
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.

Translacja adresów sieciowych dla sieci VPN

Sieć VPN udostępnia możliwość translacji adresów sieciowych określanej jako translacja 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.

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 użytkownik może próbować nawiązać połączenie z inną siecią, ale obie sieci używają adresów 10.*.*.*, co powoduje kolizję i porzucanie 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 skonfigurowania tego typu translacji VPN NAT zależy od tego, czy system jest inicjatorem połączenia VPN czy systemem odpowiadającym na to połączenie. Jeśli dany system jest inicjatorem połączenia, można tłumaczyć lokalne adresy na adresy kompatybilne z adresami partnera połączenia VPN. Jeśli dany system jest systemem odpowiadającym na połączenie, można tłumaczyć zdalne adresy partnera VPN na adresy kompatybilne 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 system działał jako system odpowiadający na swoje połączenia.

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

1. Czy firma dysponuje jednym lub wieloma systemami, do których użytkownicy mają mieć dostęp przez sieć VPN?
2. Czy wymaga się elastyczności w zakresie rzeczywistych adresów IP lokalnych systemów?
3. Czy firma dysponuje przynajmniej jednym publicznym adresem IP?

Scenariusz dotyczący używania translacji adresów sieciowych w sieci VPN stanowi przykład skonfigurowania translacji VPN NAT w celu ukrycia lokalnych adresów w modelu System i.

Instrukcje opisujące krok po kroku konfigurowanie translacji VPN NAT w systemie znajdują się w pomocy elektronicznej dostępnej z interfejsu VPN w programie System i Navigator.

Pojęcia pokrewne

“Scenariusz: używanie translacji adresów sieciowych w sieci VPN” na stronie 41
W tym scenariuszu firma zamierza wymieniać newralgiczne dane z jednym z partnerów biznesowych za pomocą

sieci VPN. W celu dodatkowego zabezpieczenia struktury sieciowej firmy, wykorzystywana ma być translacja NAT w sieci VPN, aby ukryć przed aplikacjami, do których mają dostęp partnerzy, prywatny adres IP serwera używanego w roli hosta tych aplikacji.

“Arkusz roboczy planowania połączeń ręcznych” na stronie 46
Należy wypełnić ten arkusz roboczy przed skonfigurowaniem połączenia ręcznego.

Protokół IPSec z obsługą translacji NAT oraz hermetyzacji UDP

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.

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 adres w nowym nagłówku IP zostaje poddany translacji. Następnie, kiedy pakiet dociera do celu, strona odbierająca usuwa ten dodatkowy nagłówek i pozostawia oryginalny pakiet IPSec, który przejdzie wszystkie pozostałe sprawdziany poprawności.

Hermetyzację UDP można stosować wyłącznie z protokołem IPSec ESP w trybie transportowym albo tunelowym. Ponadto system może działać tylko jako klient dla 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:

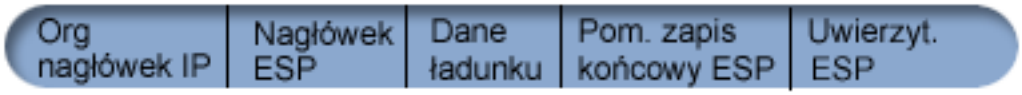
Po zastosowaniu protokołu IPSec ESP w trybie tunelowym:

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 hermetyzacji pakietu system wysyła go do partnera VPN przez port UDP 4500. Zazwyczaj obie strony połączenia VPN przeprowadziły już negocjacje IKE poprzez port UDP 500. Jeśli jednak podczas negocjacji klucza protokoły IKE wykryją translację NAT, to 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, obydwie strony połączenia muszą obsługiwać hermetyzację UDP.

Pojęcia pokrewne

"Scenariusz: sieć VPN współpracująca z zaporami firewall" na stronie 29
W tym scenariuszu duża firma ubezpieczeniowa chce nawiązać połączenie VPN pomiędzy bramą w Poznaniu a hostem w Szczecinie, gdy obydwie sieci znajdują się za zaporami firewall.

Kompresja IP

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 dwiema 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 WWW pod adresem http://www.rfc-editor.org.

Informacje pokrewne

http://www.rfc-editor.org

Sieci VPN i filtrowanie IP

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 pojęciach dotyczących filtrowania związanych z sieciami VPN.

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. Połączenie VPN może generować te reguły automatycznie. Zawsze wtedy, gdy jest to możliwe, pozwól modułowi VPN wygenerować filtry strategii. Pomaga to wyeliminować błędy, jak również eliminuje potrzebę konfigurowania reguł w oddzielnej czynności za pomocą Edytora reguł pakietów w programie System i Navigator.

Od tych zasad są jednak wyjątki. Należy przejrzeć poniższe tematy, aby dowiedzieć się więcej o innych, rzadziej używanych pojęciach dotyczących sieci VPN i filtrowania oraz technikach, które mogą mieć zastosowanie w danej sytuacji:

Pojęcia pokrewne

"Konfigurowanie reguł pakietów VPN" na stronie 52
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.

Połączenie VPN bez filtrów strategii

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.

Reguła filtrowania strategii określa adresy, protokoły i porty, które mogą korzystać z połączenia VPN, i kieruje odpowiedni ruch poprzez połączenie. W niektórych przypadkach zachodzi potrzeba skonfigurowania połączenia, które nie wymaga reguły filtrowania strategii. Na przykład reguły pakietów innych niż VPN mogą być załadowane w interfejsie, z którego będzie korzystało połączenie VPN. Zamiast więc dezaktywować aktywne reguły w tym interfejsie można skonfigurować połączenie VPN tak, aby system zarządzał dynamicznie wszystkimi filtrami dla tego połączenia. Filtr strategii dla połączenia tego typu nazywa się **dynamicznym filtrem strategii**. Aby można było korzystać z dynamicznego filtru strategii dla połączenia, muszą być spełnione następujące warunki:

- Połączenie może zostać zainicjowane tylko przez system lokalny.
- Punkty końcowe danych połączenia muszą być pojedynczymi systemami. Nie może to być podsieć ani zakres adresów.
- Dla połączenia nie można załadować żadnej reguły filtrowania strategii.

Jeśli dane połączenie spełnia te kryteria, można je skonfigurować w taki sposób, aby nie wymagało ono filtru 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 filtru strategii, znajdują się w pomocy elektronicznej dla interfejsu VPN.

Niejawne zezwolenie na ruch danych IKE

Aby w sieci VPN odbywały się negocjacje IKE, 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 niejawny.

Do nawiązania połączenia większość sieci VPN wymaga negocjacji IKE przed przetwarzaniem protokołu IPSec. 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 dopuszczałyby 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.

Scenariusze: sieć VPN

Aby poznać szczegóły techniczne i konfiguracyjne dotyczące każdego z tych podstawowych typów połączenia, należy zapoznać się z poniższymi scenariuszami.

Pojęcia pokrewne

Scenariusz QoS: Bezpieczny i przewidywalny ruch danych (sieć VPN i usługa QoS)

Informacje pokrewne

OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM e(logo)server iSeries Server with Windows 2000 VPN Clients, REDP0153

AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00

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

Scenariusz VPN: podstawowe połączenie z biurem oddziału

W tym scenariuszu firma chce ustanowić połączenie VPN między podsieciami dwóch zdalnych działów poprzez parę serwerów System i działających jako bramy VPN.

Sytuacja

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 przesyłania poufnych informacji wewnętrznych - 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.

Ważne: W omawianym scenariuszu bramy bezpieczeństwa System i są 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.

Zalety

Scenariusz ten 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.
- Użycie sieci VPN daje użytkownikom dostęp do wszystkich systemów i zasobów po obu stronach połączenia, tak jakby byli połączeni przez linię dzierżawioną lub sieć 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

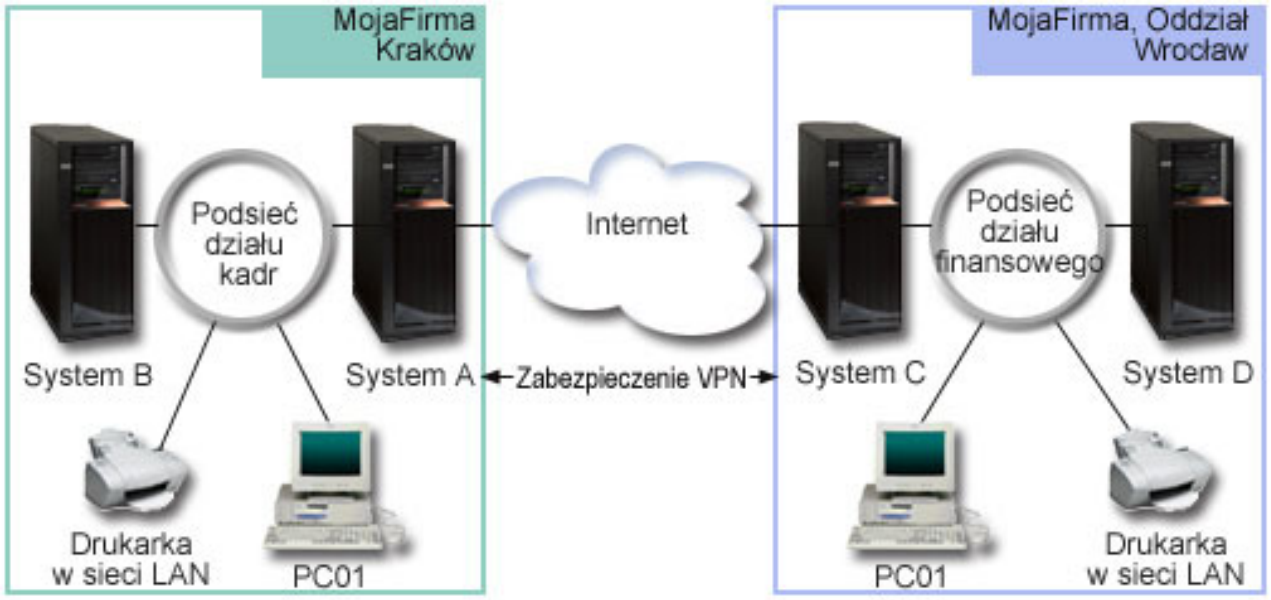
W tym scenariuszu firma MojaFirma chce ustanowić połączenie VPN między podsieciami działu kadr i działu finansowego za pośrednictwem pary serwerów System i. Oba systemy będą działać jako bramy VPN. W konfiguracji VPN bramy zarządzają kluczami i stosują protokół IPSec do danych przesyłanych tunelem. Bramy nie są punktami końcowymi danych przesyłanych w tym połączeniu.

Cele tego scenariusza są następujące:

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

Informacje szczegółowe

Poniższy rysunek ilustruje właściwości sieci firmy MojaFirma.



Dział kadr

- System A, na którym działa system operacyjny i5/OS w wersji V5R3 lub nowszej, stanowi bramę VPN działu kadr.
- 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.
- System A łączy się z Internetem za pomocą adresu IP 204.146.18.227. Stanowi on punkt końcowy połączenia. Oznacza to, że system A zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP.
- System A łączy się ze swoją podsiecią za pomocą adresu IP 10.6.11.1.
- System B jest systemem produkcyjnym w podsieci działu kadr, na którym działają standardowe aplikacje TCP/IP.

Dział finansowy

- System C, na którym działa system operacyjny i5/OS w wersji V5R3 lub nowszej, stanowi bramę VPN działu finansowego.

- 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.
- System C łączy się z Internetem za pomocą adresu IP 208.222.150.250. Stanowi on punkt końcowy połączenia. Oznacza to, że system C zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP.
- System C łączy się ze swoją podsiecią za pomocą adresu IP 10.196.8.5.

Zadania konfiguracyjne

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

Uwaga: Przed rozpoczęciem wykonywania tych zadań należy sprawdzić routing TCP/IP, aby upewnić się, że oba systemy bram mogą komunikować się ze sobą przez Internet. Dzięki temu hosty w każdej podsieci będą prawidłowo kierować do swojej bramy żądania dostępu do zdalnej podsieci.

Pojęcia pokrewne

Routing TCP/IP i równoważenie obciążenia

Informacje pokrewne

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

Wypełnianie arkuszy roboczych planowania

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: Arkusze te dotyczą systemu A; powtórz procedurę dla systemu C, zamieniając w razie potrzeby adresy IP.

Tabela 1. Wymagania systemowe

Lista kontrolna wymagań wstępnych	Odpowiedzi
Czy w systemie działa system operacyjny i5/OS w wersji V5R3 lub nowszej?	Tak
Czy opcja Digital Certificate Manager jest zainstalowana?	Tak
Czy zainstalowano program System i Access for Windows?	Tak
Czy zainstalowano program System i Navigator?	Tak
Czy zainstalowano składnik Sieć programu System i Navigator?	Tak
Czy zainstalowano program IBM TCP/IP Connectivity Utilities for i5/OS?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy w systemie 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
Czy konfiguracja firewalli lub routerów umożliwia stosowanie protokołów IKE (port UDP 500), AH i ESP?	Tak
Czy konfiguracja firewalli umożliwia przekazywanie IP?	Tak

Tabela 2. Konfiguracja VPN

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 zabezpieczenia kluczy?	Zrównoważonego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Nie: topsecretstuff
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 zabezpieczenia danych?	Zrównoważonego
Jakiego interfejsu dotyczy połączenie?	TRLINE

Konfigurowanie sieci VPN w systemie A

Aby skonfigurować system A, należy wykonać następujące czynności:

Aby skonfigurować sieć VPN w systemie A, wykonaj następujące czynności, korzystając z informacji w arkuszach roboczych.

1. W programie System i Navigator rozwiń **System A → Sieć → Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator nowych połączeń.
3. Przejrzyj stronę **Powitanie**, aby znaleźć 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 na stronę **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. Wybierz 204.146.18.227 w polu **Adres IP**.
16. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny serwer kluczy**.
17. W polu **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
18. Wpisz 208.222.150.250 w polu **Identyfikator**.
19. Wpisz topsecretstuff w polu **Wstępny klucz współużytkowany**
20. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny punkt końcowy danych**.
21. W polu **Typ identyfikatora** wybierz pozycję **Podsieć IP wersja 4**.
22. Wpisz 10.6.0.0 w polu **Identyfikator**.

23. Wpisz 255.255.0.0 w polu **Maska podsieci**.
24. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny punkt końcowy danych**.
25. Wybierz **IP wersja 4 podsieci** w polu **Typ identyfikatora**.
26. Wpisz 10.196.8.0 w polu **Identyfikator**.
27. Wpisz 255.255.255.0 w polu **Maska podsieci**.
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**.
31. Wybierz opcję **Użyj algorytmu szyfrowania RC4**.
32. Kliknij przycisk **Dalej**, aby przejść do strony **Dostępne interfejsy**.
33. Z tabeli **Wiersz** wybierz pozycję **TRLINE**.
34. Kliknij przycisk **Dalej**, aby przejść do strony **Podsumowanie**. Sprawdź, czy utworzone przez kreator obiekty są poprawne.
35. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie.
36. Po wyświetleniu okna dialogowego **Aktywowanie filtrów strategii** (Activate Policy Filters) wybierz odpowiedź **Tak, aktywuj wygenerowane filtry strategii** (Yes, activate the generated policy filters), a następnie wybierz opcję **Przepuszczaj pozostały ruch** (Permit all other traffic).
37. Kliknij przycisk **OK**, aby zakończyć konfigurowanie. W wyświetlonym oknie dialogowym zaznacz, że reguły mają być aktywowane dla wszystkich interfejsów.

Konfigurowanie sieci VPN w systemie C

Wykonaj te same czynności, co podczas konfigurowania sieci VPN w systemie A, zmieniając w razie potrzeby adresy IP. Dodatkowe wskazówki zawierają arkusze planowania.

Po zakończeniu konfigurowania bramy VPN działu finansowego połączenia będą w stanie *na żądanie*, co znaczy, że połączenie zostanie nawiązane po wysłaniu datagramów IP chronionych przez to połączenie VPN. Kolejnym krokiem jest uruchomienie serwerów VPN, o ile jeszcze nie zostały uruchomione.

Uruchamianie sieci VPN

Po skonfigurowaniu połączenia VPN w systemie A i C należy je uruchomić.

Aby uruchomić połączenie VPN, wykonaj następujące czynności:

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

Testowanie połączenia

Po zakończeniu konfigurowania obu systemów i pomyślnym uruchomieniu serwerów VPN należy przetestować połączenia, aby upewnić się, że zdalne podsieci mogą się ze sobą komunikować.

Aby przetestować połączenie, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System A → Sieć**.
2. Kliknij prawym przyciskiem myszy opcję **Konfiguracja TCP/IP** i wybierz **Narzędzia**, a następnie wybierz opcję **Ping**.
3. W oknie dialogowym **Ping z** wpisz w polu **Ping** wartość System C.
4. Kliknij przycisk **Wykonaj ping**, aby sprawdzić połączenie z systemu A do systemu C.
5. Po zakończeniu testu kliknij przycisk **OK**.

Scenariusz VPN: podstawowe połączenie pomiędzy firmami

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.

Sytuacja

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.

Załóżmy, 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 publiczny Internet, można w prosty sposób ustanowić sieć VPN, która zaspokoi potrzeby obu firm.

Cele

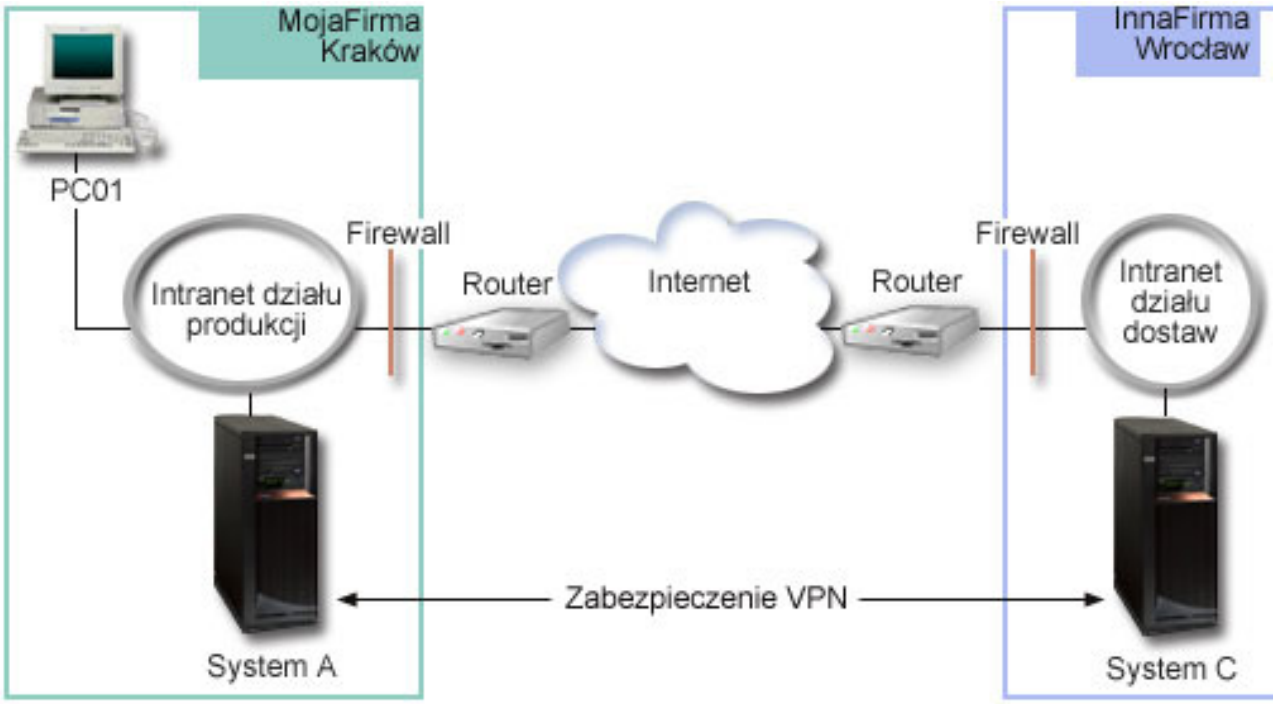
W tym scenariuszu firma MojaFirma chce nawiązać połączenie VPN pomiędzy hostem w swoim dziale podzespołów a hostem w dziale produkcji jednego ze swoich kontrahentów, firmy InnaFirma.

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.

Ważne: 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.

Informacje szczegółowe

Poniższy rysunek ilustruje schemat sieci firm MojaFirma i InnaFirma.



Sieć działu dostaw przedsiębiorstwa MojaFirma

- Na systemie A działa system operacyjny i5/OS w wersji V5R3 lub nowszej.
- System A ma adres IP 10.6.1.1. Jest to punkt końcowy zarówno połączenia, jak i danych. Oznacza to, że system A przeprowadza negocjacje IKE oraz stosuje protokół IPSec do przychodzących i wychodzących datagramów IP, jak również jest źródłem i miejscem docelowym danych przepływających przez sieć VPN.
- System A znajduje się w podsieci 10.6.0.0 z maską 255.255.0.0.
- Tylko system A może inicjować połączenie z systemem C.

Sieć działu produkcji przedsiębiorstwa InnaFirma

- Na systemie C działa system operacyjny i5/OS w wersji V5R3 lub nowszej.
- System C ma adres IP 10.196.8.6. Jest to punkt końcowy zarówno połączenia, jak i danych. Oznacza to, że system C przeprowadza negocjacje IKE oraz stosuje protokół IPSec do przychodzących i wychodzących datagramów IP, jak również jest źródłem i miejscem docelowym danych przepływających przez sieć VPN.
- System C znajduje się w podsieci 10.196.8.0 z maską 255.255.255.0.

Zadania konfiguracyjne

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

Uwaga: Przed rozpoczęciem wykonywania tych zadań należy sprawdzić routing TCP/IP, aby upewnić się, że oba systemy bram mogą komunikować się ze sobą przez Internet. Dzięki temu hosty w każdej podsieci będą prawidłowo kierować do swojej bramy żądania dostępu do zdalnej podsieci.

Pojęcia pokrewne

Routing TCP/IP i równoważenie obciążenia

Wypełnianie arkuszy roboczych planowania

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: Arkusze te dotyczą systemu A; powtórz procedurę dla systemu C, zamieniając w razie potrzeby adresy IP.

Tabela 3. Wymagania systemowe

Lista kontrolna wymagań wstępnych	**Odpowiedzi**
Czy w systemie działa system operacyjny i5/OS w wersji V5R3 lub nowszej?	Tak
Czy opcja Digital Certificate Manager jest zainstalowana?	Tak
Czy zainstalowano program System i Access for Windows?	Tak
Czy zainstalowano program System i Navigator?	Tak
Czy zainstalowano składnik Sieć programu System i Navigator?	Tak
Czy zainstalowano program IBM TCP/IP Connectivity Utilities for i5/OS?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy w systemie 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
Czy konfiguracja firewalli lub routerów umożliwia stosowanie protokołów IKE (port UDP 500), AH i ESP?	Tak
Czy konfiguracja firewalli umożliwia przekazywanie IP?	Tak

Tabela 4. Konfiguracja VPN

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 zabezpieczenia kluczy?	Zrównoważonego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Nie: topsecretstuff
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 zabezpieczenia danych?	Zrównoważonego
Jakiego interfejsu dotyczy połączenie?	TRLINE

Konfigurowanie sieci VPN w systemie A

Aby skonfigurować połączenie VPN w systemie A, należy wykonać następujące czynności:

Aby skonfigurować sieć VPN w systemie A, skorzystaj z informacji zawartych w arkuszach roboczych planowania:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator połączeń.
3. Przejrzyj stronę **Powitanie**, aby znaleźć 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 na stronę **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 reprezentujący system 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 kluczy**.
16. W polu **Typ identyfikatora** wybierz pozycję **Adres IP wersja 4**.
17. Wpisz 10.196.8.6 w polu **Identyfikator**.
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 **Aktywowanie filtrów strategii** (Activate Policy Filters) wybierz odpowiedź **Nie, reguły pakietów zostaną aktywowane później** (No, packet rules will be activated at a later time), a następnie kliknij przycisk **OK**.

Następnym krokiem jest określenie, że tylko system A może inicjować 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 przycisk **OK**, aby zapisać zmiany.

Konfigurowanie sieci VPN w systemie C

Wykonaj te same czynności, co podczas konfigurowania sieci VPN w systemie A, zmieniając w razie potrzeby adresy IP. Dodatkowe wskazówki zawierają arkusze planowania.

Po zakończeniu konfigurowania bramy VPN działu finansowego połączenia będą w stanie *na żądanie*, co znaczy, że połączenie zostanie nawiązane po wysłaniu datagramów IP chronionych przez to połączenie VPN. Kolejnym krokiem jest uruchomienie serwerów VPN, o ile jeszcze nie zostały uruchomione.

Aktywowanie reguł pakietów

Kreator VPN automatycznie tworzy reguły pakietów wymagane do poprawnego działania tego połączenia. Zanim jednak będzie można uruchomić połączenie VPN, należy je aktywować w obydwu systemach.

Aby aktywować reguły pakietów w systemie A, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **System A → Sieć → Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** (Packet Rules) i wybierz opcję **Aktywuj** (Activate). Spowoduje to otwarcie okna dialogowego **Aktywuj reguły pakietów** (Activate Packet Rules).
3. Wybierz aktywowanie 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 aktywować reguły. W tym wypadku wybierz opcję **Wszystkie interfejsy**.
5. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić zamiar weryfikacji i aktywowania 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 aktywować reguły pakietów w systemie C.

Uruchamianie połączenia

Po skonfigurowaniu połączenia VPN należy je uruchomić.

Aby uruchomić połączenie MojaFirmaDoInnaFirma z systemu A, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System 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 **Virtual Private Networking → 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*. Nawiązanie połączenia może zająć kilka minut, dlatego od czasu do czasu należy wybierać opcję odświeżania, aż status zmieni się na *Włączone* (Enabled).

Testowanie połączenia

Po zakończeniu konfigurowania obu systemów i pomyślnym uruchomieniu serwerów VPN należy przetestować połączenia, aby upewnić się, że zdalne podsieci mogą się ze sobą komunikować.

Aby przetestować połączenie, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System A → Sieć**.
2. Kliknij prawym przyciskiem myszy opcję **Konfiguracja TCP/IP** i wybierz **Narzędzia**, a następnie wybierz opcję **Ping**.
3. W oknie dialogowym **Ping z** wpisz w polu **Ping** wartość System C.
4. Kliknij przycisk **Wykonaj ping**, aby sprawdzić połączenie z systemu A do systemu C.
5. Po zakończeniu testu kliknij przycisk **OK**.

Scenariusz: zabezpieczanie dobrowolnego tunelu L2TP za pomocą protokołu IPSec

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.

Sytuacja

Załóżmy, że przedsiębiorstwo ma niewielki oddział w innym regionie. W danym dniu roboczym oddział może wymagać dostępu do informacji poufnych na temat modelu System i w korporacyjnej sieci intranet. 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 L2TP (Layer 2 Tunnel Protocol).

Ważne: W omawianym scenariuszu bramy bezpieczeństwa są podłączone bezpośrednio do Internetu. Nieuwzględnienie firewalli ma na celu uproszczenie scenariusza. Nie oznacza to jednak, że firewalle nie są konieczne. Należy liczyć się z zagrożeniami bezpieczeństwa systemu podczas każdego połączenia z Internetem.

Cele

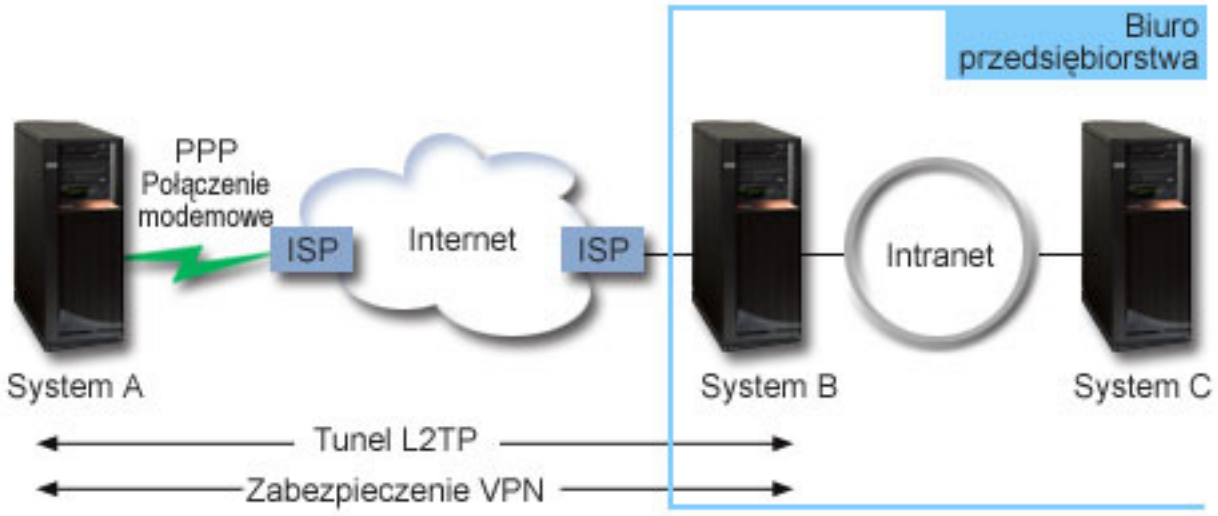
W tym scenariuszu system znajdujący się w oddziale firmy łączy się z siecią firmy poprzez system bram przez tunel L2TP zabezpieczony siecią VPN.

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.

Informacje szczegółowe

Poniższy rysunek ilustruje schemat sieci w tym scenariuszu:



System 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.

System B

- Musi mieć dostęp do aplikacji TCP/IP w systemie 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 system B zarządza kluczami i stosuje protokół IPSec do przychodzących i wychodzących datagramów IP. System B łączy się ze swoją podsiecią za pomocą adresu IP 10.6.11.1.

W terminologii protokołu L2TP *System A* działa jako inicjator L2TP, a *System B* - jako terminator L2TP.

Zadania konfiguracyjne

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

Pojęcia pokrewne

"Protokół L2TP (Layer 2 Tunneling Protocol)" na stronie 8
Połączenia korzystające z protokołu L2TP (Layer 2 Tunneling Protocol), zwane również liniami wirtualnymi, zapewniają zdalnym użytkownikom ekonomiczną metodę dostępu poprzez umożliwienie systemom sieci korporacyjnych zarządzania adresami IP przypisanymi do tych użytkowników. Ponadto połączenia L2TP używane wraz z protokołami IPSec zapewniają bezpieczny dostęp do systemów i sieci.

Informacje pokrewne

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

Konfigurowanie sieci VPN w systemie A

Aby skonfigurować połączenie VPN w systemie A, należy wykonać następujące czynności:

Aby skonfigurować sieć VPN w systemie A, skorzystaj z informacji zawartych w arkuszach roboczych planowania:

1. **Konfigurowanie strategii protokołu Internet Key Exchange**
   a. W programie System i Navigator rozwiń System A → **Sieć → Strategie IP → Sieć VPN → Strategie bezpieczeństwa IP** (System A > Network > IP Policies > Virtual Private Networking > IP Security Policies).
   b. Prawym przyciskiem myszy kliknij pozycję **Strategie Internet Key Exchange** i wybierz **Nowa strategia 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. System B korzysta z tego identyfikatora w celu zidentyfikowania systemu A, gdy ten inicjuje połączenie.
   g. Na stronie **Transformacje** (Transforms) kliknij przycisk **Dodaj** (Add), aby dodać transformacje, jakie system A proponuje systemowi B w celu zabezpieczenia klucza, oraz aby określić, czy strategia IKE korzysta z zabezpieczenia tożsamości podczas inicjowania negocjacji w fazie 1.
   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 **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 konfiguracje.
2. **Konfigurowanie strategii danych**
   a. W interfejsie VPN kliknij prawym przyciskiem myszy pozycję **Strategie danych** i wybierz opcję **Nowa strategia danych**
   b. Na stronie **Ogólne** określ nazwę strategii danych. Na przykład, zdalnyużytkownikl2tp.
   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 transformację strategii danych.
   e. Wybierz pozycję **Transport** dla trybu hermetyzacji.
   f. Kliknij przycisk **OK**, aby powrócić do strony **Transformacje**.
   g. Określ termin ważności klucza.
   h. Kliknij przycisk **OK**, aby zapisać nową strategię danych.
3. **Konfigurowanie grupy z kluczem dynamicznym**
   a. W interfejsie VPN rozwiń pozycję **Połączenia chronione**.

b. Kliknij prawym przyciskiem myszy opcję **Według grupy** i wybierz opcję **Nowa grupa 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**. Wybierz strategię danych utworzoną w sekcji **Konfigurowanie strategii danych**, zdalnyużytkownikl2tp, z listy rozwijanej **Strategia danych**.
g. Wybierz opcję **System lokalny inicjuje połączenie** (Local system initiates connection), aby wskazać, że tylko system A może inicjować połączenia z systemem B.
h. Przejdź do strony **Połączenia**. Wybierz opcję **Generuj następującą regułę filtrowania strategii dla tej grupy**. Kliknij przycisk **Edytuj**, aby zdefiniować parametry filtru 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. Wpisz 205.13.237.6 w polu **Identyfikator**.
m. Przejdź do strony **Filtr strategii - Usługi**. Wpisz 1701 w polach **Port lokalny** oraz **Port zdalny**. 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.

4. **Konfigurowanie połączenia z kluczem dynamicznym**
   a. W interfejsie VPN rozwiń pozycję **Według grupy**. Powoduje to wyświetlenie listy wszystkich grup z kluczem dynamicznym, skonfigurowanych w systemie 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. Wybierz 205.13.237.6 z listy rozwijanej **Adres IP**.
   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. Wpisz 205.13.237.6 w polu **Identyfikator**.
   j. Przejdź do strony **Usługi**. Wpisz 1701 w polach **Port lokalny** oraz **Port zdalny**. Port 1701 jest powszechnie używanym portem dla protokołu L2TP.
   k. Wybierz **UDP** z listy rozwijanej **Protokół**.
   l. Kliknij przycisk **OK**, aby utworzyć połączenie z kluczem dynamicznym.

Zadania pokrewne

“Konfigurowanie sieci VPN w systemie B” na stronie 28
Aby skonfigurować połączenie VPN w systemie B, wykonaj te same czynności, co podczas konfigurowania połączenia VPN w systemie A, zmieniając w razie potrzeby adresy IP i identyfikatory.

Konfigurowanie profilu połączenia PPP i linii wirtualnej w systemie A

Po skonfigurowaniu połączenia VPN w systemie A należy utworzyć profil PPP dla systemu A. Profil PPP nie ma powiązanej linii fizycznej; korzysta z linii wirtualnej. Dzieje się tak dlatego, że ruch PPP jest przesyłany tunelem L2TP, a sieci VPN chronią tunele L2TP.

Aby utworzyć profil połączenia PPP dla systemu A, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System 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 linii wirtualnej** wybierz pozycje **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 hosta lokalnego** (Local host name) wpisz nazwę hosta lokalnego serwera kluczy: SystemA.
14. Kliknij przycisk **OK**, aby zapisać opis nowej linii wirtualnej i powrócić do strony **Połączenia**.
15. Wpisz adres zdalnego punktu końcowego tunelu, 205.13.237.6, w polu **Adres zdalnego punktu końcowego tunelu**.
16. Wybierz opcję **Wymagana ochrona IPSec**, a następnie wybierz grupę z kluczem dynamicznym utworzoną w sekcji “Konfigurowanie sieci VPN w systemie A” na stronie 25, l2tpdocentrali, z listy rozwijanej **Nazwa grupy połączeń**.
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 podano informacji o routingu, System A będzie w stanie połączyć się ze zdalnym punktem końcowym tunelu, ale nie z jakimkolwiek innym systemem w podsieci 10.6.0.0.
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 uwierzytelnienia** wybierz opcję **Wymagaj hasła szyfrowanego (CHAP-MD5)**. W sekcji identyfikującej system lokalny wybierz opcję **Pozwól systemowi zdalnemu weryfikować tożsamość tego systemu**.
28. Wpisz nazwę użytkownika (SystemA) i hasło.
29. Kliknij przycisk **OK**, aby zapisać profil PPP.

Stosowanie grupy z kluczem dynamicznym l2tpdocentrali do profilu PPP toCorp

Po skonfigurowaniu profilu PPP należy powrócić do utworzonej wcześniej grupy z kluczem dynamicznym L2TPDoCentrali i powiązać ją z profilem PPP.

Aby grupę z kluczem dynamicznym powiązać z profilem PPP, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia → Według grupy**.
2. Prawym przyciskiem myszy kliknij grupę L2TPDoCentrali i wybierz opcję **Właściwości**.
3. Przejdź do strony **Interfejsy** i wybierz opcję **Zastosuj tę grupę** dla profilu PPP utworzonego w sekcji “Konfigurowanie profilu połączenia PPP i linii wirtualnej w systemie A” na stronie 27, doCentrali.
4. Kliknij przycisk **OK**, aby zastosować grupę L2TPDoCentrali do profilu PPP DoCentrali.

Konfigurowanie sieci VPN w systemie B

Aby skonfigurować połączenie VPN w systemie B, wykonaj te same czynności, co podczas konfigurowania połączenia VPN w systemie A, zmieniając w razie potrzeby adresy IP i identyfikatory.

Przed rozpoczęciem należy zapoznać się z poniższymi uwagami:

- Identyfikacja zdalnego serwera kluczy odbywa się według identyfikatora klucza podanego dla serwera lokalnego w systemie A. Na przykład: tojestidklucza.
- Użyj *dokładnie* tego samego wstępnego klucza współużytkowanego.
- Transformacje muszą być zgodne z transformacjami skonfigurowanymi w systemie A, w przeciwnym razie połączenie nie powiedzie się.
- Nie wybieraj opcji **Ochrona lokalnie inicjowanego tunelu L2TP** na stronie **Ogólne** grupy z kluczem dynamicznym.
- Zdalny system inicjuje połączenie.
- Zaznacz uruchamianie połączenia na żądanie.

Zadania pokrewne

“Konfigurowanie sieci VPN w systemie A” na stronie 25
Aby skonfigurować połączenie VPN w systemie A, należy wykonać następujące czynności:

Konfigurowanie profilu połączenia PPP i linii wirtualnej w systemie B

Po skonfigurowaniu połączenia VPN w systemie B należy utworzyć profil PPP dla systemu B. Profil PPP nie ma powiązanej linii fizycznej; korzysta z linii wirtualnej. Dzieje się tak dlatego, że ruch PPP jest przesyłany tunelem L2TP, a sieci VPN chronią tunele L2TP.

Aby utworzyć profil połączenia PPP dla systemu B, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System 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 DoOddzialu. 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 **DoOddzialu**. 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: SystemB.
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)** (Allow remote system to access other networks (IP forwarding)).
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 (SystemB) i hasło.
24. Kliknij przycisk **OK**, aby zapisać profil PPP.

Aktywowanie reguł pakietów

Kreator VPN automatycznie tworzy reguły pakietów wymagane do poprawnego działania tego połączenia. Zanim jednak będzie można uruchomić połączenie VPN, należy je aktywować w obydwu systemach.

Aby aktywować reguły pakietów w systemie A, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **System A → Sieć → Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** (Packet Rules) i wybierz opcję **Aktywuj** (Activate). Spowoduje to otwarcie okna dialogowego **Aktywuj reguły pakietów** (Activate Packet Rules).
3. Wybierz aktywowanie 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 aktywować reguły. W tym wypadku wybierz opcję **Wszystkie interfejsy**.
5. Kliknij przycisk **OK** w oknie dialogowym, aby potwierdzić zamiar weryfikacji i aktywowania 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 aktywować reguły pakietów w systemie B.

Scenariusz: sieć VPN współpracująca z zaporami firewall

W tym scenariuszu duża firma ubezpieczeniowa chce nawiązać połączenie VPN pomiędzy bramą w Poznaniu a hostem w Szczecinie, gdy obydwie sieci znajdują się za zaporami firewall.

Sytuacja

Duża firma ubezpieczeniowa, której oddział główny znajduje się w Szczecinie, otworzyła właśnie oddział w Poznaniu. Oddział w Poznaniu potrzebuje dostępu do bazy danych klientów bazy w Szczecinie. Firmie zależy na bezpieczeństwie przesyłanych informacji, gdyż baza danych zawiera informacje poufne klientów, takie jak nazwiska, adresy i numery telefonów. Podjęto decyzję o połączeniu obu oddziałów przez Internet za pomocą sieci VPN. Oba oddziały znajdują się za zaporami firewall i używają translacji adresów sieciowych (NAT) w celu ukrycia niezarejestrowanych prywatnych

adresów IP za zbiorem zarejestrowanych adresów IP. Jednakże istnieje kilka znanych niekompatybilności połączeń VPN z translacją NAT. Połączenie VPN usuwa pakiety przesyłane przez urządzenie NAT, ponieważ NAT zmienia adres IP pakietu, w ten sposób unieważniając ten pakiet. Można jednak zastosować połączenie VPN z translacją NAT, jeśli zaimplementowana będzie hermetyzacja UDP.

W tym scenariuszu prywatny adres IP z sieci w Poznaniu jest umieszczany w nowym nagłówku IP i tłumaczony podczas przechodzenia przez zaporę firewall C (patrz rysunek). Następnie, gdy pakiet dotrze do zapory firewall D, docelowy adres IP zostanie przetłumaczony na adres IP systemu E, dzięki czemu pakiet zostanie przekazany do tego systemu. Na koniec, gdy pakiet dotrze do systemu E, nagłówek UDP zostanie usunięty, przez co pozostanie pierwotny pakiet IPSec, który teraz przejdzie pomyślnie sprawdzanie i zapewni bezpieczne połączenie VPN.

Cele

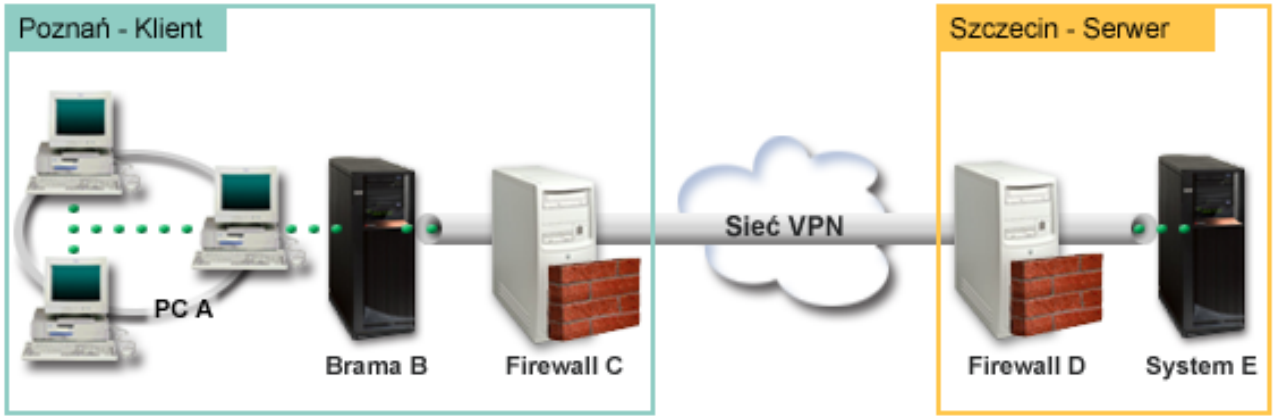
W tym scenariuszu duża firma ubezpieczeniowa chce nawiązać połączenie VPN pomiędzy bramą w Poznaniu (klient) a hostem w Szczecinie (serwer), gdy obydwie sieci znajdują się za zaporą firewall.

Cele tego scenariusza są następujące:

- Brama oddziału w Poznaniu zawsze inicjuje połączenie z hostem w Szczecinie.
- Sieć VPN musi chronić cały ruch danych pomiędzy bramą w Poznaniu a hostem w Szczecinie.
- Wszyscy użytkownicy w bramie w Poznaniu mają dostęp do bazy danych serwera System i znajdującej się w sieci w Szczecinie przez połączenie VPN.

Informacje szczegółowe

Poniższy rysunek ilustruje schemat sieci w tym scenariuszu:



Sieć Poznań - klient

- W bramie B działa system operacyjny i5/OS w wersji V5R4 lub nowszej.
- Brama B łączy się z Internetem przy użyciu adresu IP 214.72.189.35 i jest punktem końcowym połączenia tunelu VPN. Brama B przeprowadza negocjacje IKE i stosuje hermetyzację UDP do wychodzących datagramów IP.
- Brama B i komputer A są w podsieci 10.8.11.0 z maską 255.255.255.0.
- Komputer A jest systemem źródłowym i docelowym dla danych przechodzących przez połączenie VPN, dlatego jest punktem końcowym danych w tunelu VPN.
- Tylko brama B może inicjować połączenie z systemem E.
- Zapora firewall C ma regułę Masq NAT z publicznym adresem IP 129.42.105.17, która ukrywa adres IP bramy B.

Sieć Szczecin - serwer

- W systemie E działa system operacyjny i5/OS w wersji V5R4 lub nowszej.

- System E ma adres IP 56.172.1.1.
- System E jest w tym scenariuszu systemem odpowiadającym.
- Zapora firewall D ma adres IP 146.210.18.51.
- Zapora firewall D ma regułę Static NAT, która odwzorowuje publiczny adres IP (146.210.18.15) na prywatny adres IP systemu E (56.172.1.1). Dlatego z punktu widzenia klienta adres IP systemu E jest publicznym adresem IP (146.210.18.51) zapory firewall D.

Zadania konfiguracyjne

Pojęcia pokrewne

"Zarządzanie kluczami" na stronie 6
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 IPSec z obsługą translacji NAT oraz hermetyzacji UDP" na stronie 10
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.

Wypełnianie arkuszy roboczych 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: Dla bramy B i systemu E używa się oddzielnych arkuszy roboczych.

Tabela 5. Wymagania systemowe

Lista kontrolna wymagań wstępnych	**Odpowiedzi**
Czy używany system operacyjny to i5/OS w wersji V5R4 lub nowszej?	Tak
Czy opcja Digital Certificate Manager jest zainstalowana?	Tak
Czy zainstalowano program System i Access for Windows?	Tak
Czy zainstalowano program System i Navigator?	Tak
Czy zainstalowano składnik Sieć programu System i Navigator?	Tak
Czy zainstalowano program IBM TCP/IP Connectivity Utilities for i5/OS?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy w systemie 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
Czy konfiguracja zapór firewall i routerów umożliwia ruch przez port 450 dla negocjacji klucza? Zazwyczaj obie strony połączenia VPN przeprowadzają negocjacje IKE poprzez port UDP 500, gdy protokół IKE wykryje, że pakiety NAT są przesyłane poprzez port 4500.	Tak
Czy konfiguracja firewalli umożliwia przekazywanie IP?	Tak

Tabela 6. Konfiguracja bramy B

Informacje potrzebne do skonfigurowania połączenia VPN dla bramy B	**Odpowiedzi**
Jakiego typu połączenie jest tworzone?	brama-inny host
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	brPozDoHostSzcze

Tabela 6. Konfiguracja bramy B (kontynuacja)

Informacje potrzebne do skonfigurowania połączenia VPN dla bramy B	**Odpowiedzi**
Jakiego typu ochrony i wydajności systemu wymaga się do zabezpieczenia kluczy?	Zrównoważonego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Nie: topsecretstuff
Jaki jest identyfikator lokalnego serwera kluczy?	Adres IP: 214.72.189.35
Jaki jest identyfikator lokalnego punktu końcowego danych?	Podsieć: 10.8.11.0 Maska: 255.255.255.0
Jaki jest identyfikator zdalnego serwera kluczy?	Adres IP: 146.210.18.51
Jaki jest identyfikator zdalnego punktu końcowego danych?	Adres IP: 146.210.18.51
Jakie protokoły i jakie porty mają być dostępne dla połączenia?	Dowolne
Jakiego typu ochrony i wydajności systemu wymaga się do zabezpieczenia danych?	Zrównoważonego
Jakiego interfejsu dotyczy połączenie?	TRLINE

Tabela 7. Konfiguracja systemu E

Informacje potrzebne do skonfigurowania połączenia VPN dla systemu E	**Odpowiedzi**
Jakiego typu połączenie jest tworzone?	host-do-innej bramy
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	brPozDoHostSzcze
Jakiego typu ochrony i wydajności systemu wymaga się do zabezpieczenia kluczy?	Najwyższego
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	Nie: topsecretstuff
Jaki jest identyfikator lokalnego serwera kluczy?	Adres IP: 56.172.1.1
Jaki jest identyfikator zdalnego serwera kluczy? **Uwaga:** Jeśli adres IP zapory firewall C jest nieznany, można użyć wartości *ANYIP jako identyfikatora zdalnego serwera kluczy.	Adres IP: 129.42.105.17
Jaki jest identyfikator zdalnego punktu końcowego danych?	Podsieć: 10.8.11.0 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 zabezpieczenia danych?	Najwyższego
Jakiego interfejsu dotyczy połączenie?	TRLINE

Odsyłacze pokrewne

Doradca w zakresie planowania połączeń VPN

Konfigurowanie sieci VPN w bramie B

Aby skonfigurować połączenie VPN w bramie B, należy wykonać następujące czynności.

Aby skonfigurować sieć VPN w bramie B, skorzystaj z informacji zawartych w arkuszach roboczych planowania:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator połączeń.
3. Przejrzyj stronę **Powitanie**, aby znaleźć informacje o obiektach tworzonych przez kreator.
4. Kliknij przycisk **Dalej**, aby przejść do strony **Nazwa połączenia**.
5. W polu **Nazwa** wpisz brPozDoHostSzcze.
6. Opcjonalnie: Wprowadź opis tej grupy połączeń.
7. Kliknij przycisk **Dalej**, aby przejść do strony **Scenariusz połączenia**.
8. Wybierz opcję **Połączenie bramy użytkownika z innym hostem**.

9. Kliknij przycisk **Dalej**, aby przejść na stronę **Strategia protokołu IKE**.
10. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz **Równoważ ochronę i wydajność**.

    Uwaga: Jeśli pojawi się komunikat o błędzie o treści ″Nie można przetworzyć żądania certyfikatu″, można je zignorować, gdyż certyfikaty nie są używane do wymiany klucza.
11. Opcjonalnie: Jeśli zainstalowane są certyfikaty, wyświetlona zostanie strona **Certyfikat dla lokalnego punktu końcowego połączenia**. Wybierz opcję Nie, aby wskazać, że do uwierzytelniania tego połączenia będzie używany certyfikat.
12. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny serwer kluczy**.
13. Wybierz **IP wersja 4** w polu **Typ identyfikatora**.
14. Wybierz 214.72.189.35 w polu **Adres IP**.
15. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny serwer kluczy**.
16. Wybierz **Adres IP wersja 4** w polu **Typ identyfikatora**.
17. Wpisz 146.210.18.51 w polu **Identyfikator**.

    Uwaga: Brama B inicjuje połączenie ze statyczną siecią NAT. W celu wprowadzenia pojedynczego numeru IP dla zdalnego klucza należy określić wymianę kluczy trybu głównego. Główny tryb wymiany klucza jest wybierany domyślnie, gdy tworzone jest połączenie za pomocą kreatora połączenia VPN. Jeśli w tej sytuacji będzie użyty agresywny tryb uzgadniania, należy dla klucza zdalnego podać identyfikator zdalny z typem innym niż IPV4.
18. Wpisz topsecretstuff w polu **Wstępny klucz współużytkowany**
19. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny punkt końcowy danych**.
20. W polu **Typ identyfikatora** wybierz pozycję **Podsieć IP wersja 4**.
21. Wpisz 10.8.0.0 w polu **Identyfikator**.
22. Wpisz 255.255.255.0 w polu **Maska podsieci**.
23. Kliknij przycisk **Dalej**, aby przejść do strony **Usługi danych**.
24. Zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**, aby przejść do strony Strategia danych.
25. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz **Równoważ ochronę i wydajność**.
26. Kliknij przycisk **Dalej**, aby przejść do strony **Dostępne interfejsy**.
27. Wybierz **TRLINE** z tabeli Wiersz.
28. Kliknij przycisk **Dalej**, aby przejść do strony **Podsumowanie**.
29. Sprawdź, czy utworzone przez kreator obiekty są poprawne.
30. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie.
31. Gdy pojawi się okno dialogowe **Aktywowanie filtrów strategii**, wybierz opcję **Tak**, aktywuj wygenerowane filtry strategii, a następnie wybierz opcję **Zezwalaj na pozostały ruch**.
32. Kliknij przycisk **OK**, aby zakończyć konfigurowanie.

Konfigurowanie sieci VPN w systemie E

Aby skonfigurować połączenie VPN w systemie E, należy wykonać następujące czynności.

Aby skonfigurować sieć VPN w systemie E, skorzystaj z informacji zawartych w arkuszach roboczych planowania:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Nowe połączenie**, aby uruchomić Kreator połączeń.
3. Przejrzyj stronę **Powitanie**, aby znaleźć informacje o obiektach tworzonych przez kreator.
4. Kliknij przycisk **Dalej**, aby przejść do strony **Nazwa połączenia**.
5. W polu **Nazwa** wpisz brPozDoHostSzcze.
6. Opcjonalnie: Wprowadź opis tej grupy połączeń.
7. Kliknij przycisk **Dalej**, aby przejść do strony **Scenariusz połączenia**.

8. Wybierz opcję **Połączenie hosta użytkownika z inną bramą**
9. Kliknij przycisk **Dalej**, aby przejść na stronę **Strategia protokołu IKE**.
10. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz opcję **Równoważ ochronę i wydajność**.

    Uwaga: Jeśli pojawi się komunikat o błędzie o treści ″Nie można przetworzyć żądania certyfikatu″, można je zignorować, gdyż certyfikaty nie są używane do wymiany klucza.
11. Opcjonalnie: Jeśli zainstalowane są certyfikaty, wyświetlona zostanie strona **Certyfikat dla lokalnego punktu końcowego połączenia**. Wybierz opcję Nie, aby wskazać, że do uwierzytelniania tego połączenia będzie używany certyfikat.
12. Kliknij przycisk **Dalej**, aby przejść do strony **Lokalny serwer kluczy**.
13. Wybierz **Adres IP wersja 4** w polu **Typ identyfikatora**.
14. Wybierz 56.172.1.1 w polu **Adres IP**.
15. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny serwer kluczy**.
16. Wybierz **Adres IP wersja 4** w polu **Typ identyfikatora**.
17. Wpisz 129.42.105.17 w polu **Identyfikator**.

    Uwaga: Jeśli adres IP zapory firewall C jest nieznany, można użyć wartości *ANYIP jako identyfikatora zdalnego serwera kluczy.
18. Wpisz topsecretstuff w polu **Wstępny klucz współużytkowany**
19. Kliknij przycisk **Dalej**, aby przejść do strony **Zdalny punkt końcowy danych**.
20. W polu **Typ identyfikatora** wybierz pozycję **Podsieć IP wersja 4**.
21. Wpisz 10.8.11.0 w polu **Identyfikator**.
22. Wpisz 255.255.255.0 w polu **Maska podsieci**.
23. Kliknij przycisk **Dalej**, aby przejść do strony **Usługi danych**.
24. Zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**, aby przejść do strony Strategia danych.
25. Wybierz opcję **Utwórz nową strategię**, a następnie wybierz opcję **Równoważ ochronę i wydajność**.
26. Kliknij przycisk **Dalej**, aby przejść do strony **Dostępne interfejsy**.
27. Wybierz **TRLINE** z tabeli Wiersz.
28. Kliknij przycisk **Dalej**, aby przejść do strony **Podsumowanie**.
29. Sprawdź, czy utworzone przez kreator obiekty są poprawne.
30. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie.
31. Gdy pojawi się okno dialogowe **Aktywowanie filtrów strategii**, wybierz opcję **Tak**, aktywuj wygenerowane filtry strategii, a następnie wybierz opcję **Zezwalaj na pozostały ruch**.
32. Kliknij przycisk **OK**, aby zakończyć konfigurowanie.

Uruchamianie połączenia

Po skonfigurowaniu połączenia VPN w systemie E należy je uruchomić.

Aby potwierdzić, że połączenie brPozDoHostSzcze w systemie E jest aktywne, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **System E → Sieć → Bezpieczne połączenia → Wszystkie połączenia**.
2. Wyświetl **brPozDoHostSzcze** i sprawdź, czy w polu **Status** wyświetlone są wartości *Bezczynny* lub *Na żądanie*.

Aby uruchomić połączenie brPozDoHostSzcze z bramy B, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń **Brama B → Sieć → Strategie IP**.
2. Jeśli serwer VPN nie jest uruchomiony, kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Uruchom**.
3. Rozwiń **Virtual Private Networking → Połączenia chronione**.
4. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.

5. Kliknij prawym przyciskiem myszy pozycję **brPozDoHostSzcze** i wybierz opcję **Uruchom**.
6. Z menu **Widok** wybierz opcję **Odśwież**. Jeśli połączenie zostanie pomyślnie uruchomione, w polu **Status** zamiast wartości *Uruchamianie* lub *Na żądanie* wyświetlona zostanie wartość *Aktywowano*. Nawiązanie połączenia może zająć trochę czasu, dlatego należy okresowo wybierać opcję odświeżania, aż status zmieni się na *Włączone* (Enabled).

Testowanie połączenia

Po zakończeniu konfigurowania bramy B i systemu E oraz pomyślnym uruchomieniu serwerów VPN należy przetestować połączenia, aby upewnić się, że oba systemy mogą się ze sobą komunikować.

Aby przetestować połączenia, należy wykonać następujące czynności:

1. Znajdź system w sieci komputera A i otwórz sesję Telnet.
2. Podaj publiczny adres IP systemu E, czyli 146.210.18.51.
3. Podaj inne informacje o wpisaniu się, jeśli to konieczne. Jeśli pojawia się ekran wpisania się, oznacza to, że połączenie działa poprawnie.

Scenariusz: połączenie VPN ze zdalnymi użytkownikami

Aby włączyć połączenia zdalne, administrator musi skonfigurować połączenie VPN ze zdalnymi użytkownikami.

Następujące zadania przedstawiają, jak administrator konfiguruje połączenie VPN ze zdalnymi użytkownikami.

Wypełnianie arkuszy roboczych planowania dla połączenia VPN z oddziału do zdalnych sprzedawców

Administrator działu sprzedaży w oddziale korzysta z doradcy w zakresie planowania sieci VPN w celu utworzenia dynamicznych arkuszy roboczych planowania pomagających pracownikom skonfigurować sieć VPN w systemach i zdalnych stacjach roboczych.

Doradca w zakresie planowania sieci VPN jest interaktywnym narzędziem, które zadaje konkretne pytania dotyczące wymagań względem sieci VPN. Na podstawie odpowiedzi doradca tworzy dla danego środowiska dostosowany arkusz roboczy planowania, którego można użyć podczas konfigurowania połączenia VPN. Arkusza tego można następnie użyć podczas konfigurowania sieci VPN w systemie. Każdy z następujących arkuszy roboczych planowania jest generowany za pomocą doradcy w zakresie planowania sieci VPN i służy do skonfigurowania sieci VPN za pomocą kreatora nowego połączenia VPN, zawartego w programie System i Navigator.

Tabela 8. Arkusz roboczy planowania połączenia VPN między działem sprzedaży w oddziale a zdalnymi sprzedawcami

O co pyta kreator sieci VPN	**Co zaleca doradca sieci VPN**
Jak chcesz nazwać tę grupę połączenia?	SprzedazdoZdalnych
Jakiego typu grupę połączenia chcesz utworzyć?	Wybierz opcję **Połącz lokalny host z innym hostem** (Connect your host to another host).
Jakiej strategii IKE (Internet Key Exchange) chcesz użyć do zabezpieczenia klucza?	Wybierz **Utwórz nową strategię** (Create a new policy), a następnie wybierz **Najwyższa ochrona, najniższa wydajność** (highest security, lowest performance).
Czy używane są certyfikaty?	Wybierz opcję **Nie**.

Tabela 8. Arkusz roboczy planowania połączenia VPN między działem sprzedaży w oddziale a zdalnymi sprzedawcami (kontynuacja)

O co pyta kreator sieci VPN	Co zaleca doradca sieci VPN
Wpisz identyfikator, który będzie odpowiadał lokalnemu serwerowi kluczy dla tego połączenia.	Typ identyfikatora: **adres IP wersja 4**, adres IP: **192.168.1.2**. Dla adresu IPv6 - typ identyfikatora: **adres IP wersja 6**, adres IP: **2001:DB8::2** **Uwaga:** Adresy IP użyte w tym scenariuszu stanowią jedynie przykład. Nie odzwierciedlają one schematu adresowania IP i nie należy ich używać w jakiejkolwiek rzeczywistej konfiguracji. Wykonując te zadania, należy używać własnych adresów IP.
Jaki jest identyfikator serwera kluczy, z którym chcesz się połączyć?	Typ identyfikatora: **dowolny adres IP**, **Wstępny klucz współużytkowany**: kluczmojejfirmy. **Uwaga:** Wstępny klucz współużytkowany jest 32-znakowym łańcuchem tekstowym, którego sieć VPN i5/OS używa do uwierzytelniania połączenia oraz ustanawiania kluczy zabezpieczających dane. Ogólnie rzecz biorąc, należy traktować wstępny klucz współużytkowany w taki sam sposób, jak hasło.
Jakie są porty i protokoły danych, które to połączenie będzie zabezpieczać?	**Port lokalny**: 1701, **Port zdalny**: dowolny port, **Protokół**: UDP
Jakiej strategii danych chcesz użyć do zabezpieczenia danych?	Wybierz **Utwórz nową strategię** (Create a new policy), a następnie wybierz **Najwyższa ochrona, najniższa wydajność** (highest security, lowest performance).
Sprawdź interfejsy w systemie lokalnym, do których będzie mieć zastosowanie to połączenie.	ETHLINE (Dział sprzedaży w oddziale)

Konfigurowanie profilu terminatora L2TP dla systemu A

Aby skonfigurować połączenia zdalne ze zdalnymi stacjami roboczymi, należy skonfigurować system A, tak aby akceptował połączenia przychodzące od tych klientów.

Aby skonfigurować profil terminatora L2TP dla systemu A, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń ***System A*** → **Sieć** → **Usługi zdalnego dostępu** (System A > Sieć > Remote Access Services).
2. Kliknij prawym przyciskiem myszy **Profile połączenia odbiorcy** (Receiver Connection Profiles), aby ustawić system A jako serwer odbierający połączenia przychodzące od zdalnych użytkowników, i wybierz opcję **Nowy profil** (New Profile).
3. Na stronie Konfiguracja (Setup) wybierz następujące opcje:
   - **Typ protokołu** (Protocol type): PPP
   - **Typ połączenia** (Connection type): L2TP (linia wirtualna)

Uwaga: W polu **Tryb pracy** (Operating mode) powinna zostać automatycznie wyświetlona wartość **Terminator (serwer sieciowy)** (Terminator (network server).

- **Typ usługi linii** (Line service type): pojedyncza linia

4. Kliknij przycisk **OK**. Spowoduje to otwarcie strony Właściwości profilu nowego połączenia punkt z punktem (New Point-to-Point Profile Properties).
5. Na karcie **Ogólne** (General) wypełnij następujące pola:
   - **Nazwa** (Name): MYCOL2TP
   - Jeśli profil ma być automatycznie uruchamiany wraz z protokołem TCP, wybierz opcję **Uruchamiaj profil z TCP** (Start profile with TCP).
6. Na karcie **Połączenie** (Connection) wybierz **192.168.1.2** (**2001:DB8::2** w IPv6) dla opcji **Adres IP lokalnego punktu końcowego tunelu** (Local tunnel endpoint IP address).

   Ważne: Adresy IP użyte w tym scenariuszu stanowią jedynie przykład. Nie odzwierciedlają one schematu adresowania IP i nie należy ich używać w jakiejkolwiek rzeczywistej konfiguracji. Wykonując te zadania, należy używać własnych adresów IP.
7. Wybierz wartość **MYCOL2TP** dla opcji **Nazwa linii wirtualnej** (Virtual line name). Spowoduje to otwarcie strony właściwości nowego połączenia L2TP.
8. Na stronie Uwierzytelnianie (Authentication) jako nazwę hosta wpisz systema. Kliknij przycisk **OK**. Spowoduje to powrót do strony Połączenie (Connection).
9. Na stronie Połączenie wybierz następujące opcje i jako **Maksymalna liczba połączeń** (Maximum number of connections) wpisz 25.
   a. Kliknij zakładkę **Uwierzytelnianie** (Authentication) i wybierz opcję **Wymagaj, aby ten system weryfikował tożsamość systemu zdalnego** (Require this system to verify the identity of the remote system).
   b. Wybierz opcję **Uwierzytelniaj lokalnie za pomocą listy sprawdzania** (Authenticate locally with validation list).
   c. W polu **Nazwa listy sprawdzania** (Validation list name) wpisz QL2TP i kliknij przycisk **Nowy** (New).
10. Na stronie Lista sprawdzania (Validation list) wybierz **Dodaj** (Add).
11. Dodaj nazwy użytkowników i hasła dla każdego pracownika zdalnego. Kliknij przycisk **OK**.
12. Na stronie Potwierdzenie hasła (Password confirmation) ponownie wpisz hasło dla każdego z tych pracowników. Kliknij przycisk **OK**.
13. Na stronie Ustawienia TCP/IP (TCP/IP Setting) wybierz 10.1.1.1 (2001:DA8::1 w przypadku IPv6) jako **Lokalny adres IP** (Local IP address).
14. W polu **Metoda przypisania adresu IP** (IP address assignment method) wybierz opcję **Pula adresów** (Address pool).
15. W polu **Początkowy adres IP** (Starting IP address) wpisz 10.1.1.100, a w polu **Liczba adresów** (Number of addresses) wpisz 49. W przypadku adresów IPv6 w polu **Początkowy adres IP** wpisz 2001:DA8::1:1, a w polu **Liczba adresów** wpisz 65535.
16. Wybierz opcję **Pozwól zdalnemu systemowi na dostęp do innych sieci (przekazywanie IP)** (Allow remote system to access other networks (IP forwarding)). Kliknij przycisk **OK**.

Uruchamianie profilu połączenia odbiorcy

Po skonfigurowaniu profilu połączenia odbiorcy L2TP (Layer Two Tunneling Protocol) dla systemu A administrator musi uruchomić to połączenie, aby nasłuchiwało przychodzących żądań od klientów zdalnych.

Uwaga: Może zostać wyświetlony komunikat o błędzie, że podsystem QUSRWRK nie jest uruchomiony. Komunikat ten występuje podczas próby uruchomienia profilu połączenia odbiorcy. Aby uruchomić podsystem QUSRWRK, należy wykonać następujące czynności:

1. W interfejsie znakowym wpisz strsbs.
2. Na ekranie Uruchomienie podsystemu (Start Subsystem) wpisz QUSRWRK w polu **Opis podsystemu** (Subsystem description).

Aby uruchomić profil połączenia odbiorcy dla klientów zdalnych, należy wykonać następujące czynności:

1. W programie System i Navigator wybierz opcję **Odśwież** (Refresh) z menu **Widok** (View). Spowoduje to odświeżenie instancji programu System i Navigator.
2. W programie System i Navigator rozwiń ***System A*** **→ Sieć → Usługi zdalnego dostępu** (System A > Sieć > Remote Access Services).
3. Dwukrotnie kliknij **Profile połączenia odbiorcy** (Receiver Connection Profiles), kliknij prawym przyciskiem myszy **MYCOL2TP** i wybierz opcję **Uruchom** (Start).
4. Zostanie wyświetlone pole **Status** z wartością **Oczekiwanie na żądania połączenia** (Waiting for connection requests).

Konfigurowanie połączenia VPN w systemie A dla klientów zdalnych

Po skonfigurowaniu i uruchomieniu profilu połączenia odbiorcy L2TP (Layer Two Tunneling Protocol) dla systemu A administrator musi skonfigurować sieć VPN, aby zabezpieczyć połączenie między klientami zdalnymi a siecią w dziale sprzedaży oddziału.

Aby skonfigurować sieć VPN dla klientów zdalnych, należy wykonać następujące czynności:

Ważne: Adresy IP użyte w tym scenariuszu stanowią jedynie przykład. Nie odzwierciedlają one schematu adresowania IP i nie należy ich używać w jakiejkolwiek rzeczywistej konfiguracji. Wykonując te zadania, należy używać własnych adresów IP.

1. W programie System i Navigator rozwiń ***System A*** **→ Sieć → Strategie IP** (System A > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** (Virtual Private Networking) i wybierz opcję **Nowe połączenie** (New Connection), aby uruchomić Kreator nowych połączeń VPN. Przejrzyj stronę powitalną, aby znaleźć informacje o obiektach, które tworzy kreator.
3. Kliknij przycisk **Dalej**, aby przejść do strony Nazwa połączenia (Connection Name).
4. W polu **Nazwa** (Name) wpisz SprzedazdoZdalnych.
5. Opcjonalne: Podaj opis tej grupy połączeń. Kliknij przycisk **Dalej**.
6. Na stronie Scenariusz połączenia (Connection Scenario) wybierz pozycję **Połącz lokalny host z innym hostem** (Connect your host to another host). Kliknij przycisk **Dalej**.
7. Na stronie Strategia IKE (Internet Key Exchange Policy) wybierz **Utwórz nową strategię** (Create a new policy), a następnie wybierz **Najwyższa ochrona, najniższa wydajność** (Highest security, lowest performance). Kliknij przycisk **Dalej**.
8. Na stronie Certyfikat dla lokalnego punktu końcowego połączenia (Certificate for Local Connection Endpoint) wybierz opcję **Nie** (No). Kliknij przycisk **Dalej**.
9. Na stronie Lokalny serwer kluczy (Local Key Server) jako typ identyfikatora wybierz **Adres IP wersja 4** (Version 4 IP address). Powiązanym adresem IP powinien być 192.168.1.2. Kliknij przycisk **Dalej**. W przypadku adresu IPv6 na stronie Lokalny serwer kluczy jako typ identyfikatora wybierz **Adres IP wersja 6** (Version 6 IP address). Powiązanym adresem IP powinien być 2001:DB8::2. Kliknij przycisk **Dalej**.
10. Na stronie Zdalny serwer kluczy w polu **Typ identyfikatora** (Identifier type) wybierz pozycję **Dowolny adres IP** (Any IP address). W polu **Wstępny klucz współużytkowany** (Pre-shared key) wpisz kluczmojejfirmy. Kliknij przycisk **Dalej**.
11. Na stronie Usługi danych (Data Services) wpisz 1701 dla portu lokalnego. Następnie wybierz wartość 1701 dla portu zdalnego i **UDP** dla protokołu. Kliknij przycisk **Dalej**.
12. Na stronie Strategia danych (Data Policy) wybierz **Utwórz nową strategię** (Create a new policy), a następnie wybierz **Najwyższa ochrona, najniższa wydajność** (Highest security, lowest performance). Kliknij przycisk **Dalej**.
13. Na stronie Stosowane interfejsy (Applicable Interfaces) wybierz **ETHLINE**. Kliknij przycisk **Dalej**.
14. Na stronie Podsumowanie (Summary) sprawdź, czy utworzone przez kreator obiekty są poprawne.
15. Kliknij przycisk **Zakończ**, aby zakończyć konfigurowanie. Po wyświetleniu okna dialogowego Aktywowanie filtrów strategii (Activate Policy Filters) wybierz odpowiedź **Nie, reguły pakietów zostaną aktywowane później** (No, packet rules will be activated at a later time). Kliknij przycisk **OK**.

Aktualizacja strategii VPN dla połączeń zdalnych z klientów Windows XP i Windows 2000

Ponieważ kreator tworzy standardowe połączenie, które może być używane w większości konfiguracji sieci VPN, należy zaktualizować wygenerowane przez niego strategie, aby zapewnić współdziałanie klientów Windows XP i Windows 2000.

Aby zaktualizować strategie VPN, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń ***System A*** → **Sieć** → **Strategie IP** → **Sieć VPN** → **Strategie bezpieczeństwa IP** (System A > Network > IP Policies > Virtual Private Networking > IP Security Policies).
2. Dwukrotnie kliknij **Strategie IKE** (Internet Key Exchange Policies), kliknij prawym przyciskiem myszy **Dowolny adres IP** (Any IP address) i wybierz opcję **Właściwości** (Properties).
3. Na stronie Transformacje (Transform) kliknij przycisk **Dodaj** (Add).
4. Na stronie Dodaj transformację IKE (Add Internet Key Exchange Transform) wybierz następujące opcje:
   - **Metoda uwierzytelniania** (Authentication method): wstępny klucz współużytkowany
   - **Algorytm mieszający** (Hash algorithm): MD5
   - **Algorytm szyfrowania** (Encryption algorithm): DES-CBC
   - **Grupa Diffie-Hellman** (Diffie-Hellman group): grupa 1
5. Kliknij przycisk **OK**.
6. W programie System i Navigator rozwiń ***System A*** → **Sieć** → **Strategie IP** → **Sieć VPN** → **Strategie bezpieczeństwa IP** (System A > Network > IP Policies > Virtual Private Networking > IP Security Policies).
7. Dwukrotnie kliknij **Strategie danych** (Data Policies), kliknij prawym przyciskiem myszy **SprzedazdoZdalnych** i wybierz opcję **Właściwości** (Properties).
8. Na stronie Ogólne usuń zaznaczenie pola **Metoda utajniania Diffie-Hellman** (Use Diffie-Hellman perfect forward secrecy).
9. Wybierz opcję **Propozycja ESP** (ESP Proposal) i kliknij przycisk **Edycja** (Edit).
10. Na stronie Propozycja strategii danych (Data Policy Proposal) zmień opcje w następujący sposób:
    - **Tryb hermetyzacji** (Encapsulation mode): transport
    - **Czas ważności klucza** (Key expiration): 15 minut
    - **Wygaśnięcie po osiągnięciu wielkości** (Expire at size limit): 100000
11. Na stronie Transformacje (Transform) kliknij przycisk **Dodaj** (Add).
12. Na stronie Dodaj transformację strategii danych wybierz następujące opcje:
    - **Protokół** (Protocol): Encapsulating security payload (ESP)
    - **Algorytm uwierzytelniania** (Authentication algorithm): MD5
    - **Algorytm szyfrowania** (Encryption algorithm): DES-CBC
13. Dwukrotnie kliknij przycisk **OK**.

Aktywowanie reguł filtrowania

Kreator automatycznie tworzy reguły pakietów wymagane do poprawnego działania tego połączenia. Zanim jednak będzie można uruchomić połączenie VPN, należy je aktywować w obydwu systemach.

Aby aktywować reguły filtrowania w systemie A, wykonaj następujące czynności:

Ważne: Adresy IP użyte w tym scenariuszu stanowią jedynie przykład. Nie odzwierciedlają one schematu adresowania IP i nie należy ich używać w jakiejkolwiek rzeczywistej konfiguracji. Wykonując te zadania, należy używać własnych adresów IP.

1. W programie System i Navigator rozwiń ***System A*** → **Sieć** → **Strategie IP** (System A > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy pozycję **Reguły pakietów** (Packet Rules) i wybierz opcję **Aktywuj reguły** (Activate Rules).

3. Na stronie Aktywuj reguły pakietów wybierz opcję **aktywuj tylko reguły wygenerowane przez VPN** (activate only the VPN generated rules), a jako interfejs, na którym chcesz aktywować te reguły filtrowania, wybierz **ETHLINE**. Kliknij przycisk **OK**.

Zanim zdalni użytkownicy będą mogli skonfigurować swoje stacje robocze Windows XP, administrator musi podać im następujące informacje, aby mogli skonfigurować swoją stronę połączenia. Każdemu użytkownikowi zdalnemu należy przekazać następujące informacje:

- nazwa wstępnego klucza współużytkowanego: kluczmojejfirmy;
- adres IP systemu A: 192.168.1.2 (2001:DB8::2 w IPv6);
- nazwa użytkownika i hasło dla połączenia.

Uwaga: Dane te zostały utworzone w momencie, gdy administrator dodał nazwę użytkownika i hasła do listy sprawdzania podczas konfigurowania profilu terminatora protokołu L2TP (Layer Two Tunneling Protocol).

Konfigurowanie sieci VPN na kliencie Windows XP

Procedura ta służy do konfigurowania sieci VPN na kliencie Windows XP.

Zdalni użytkownicy w firmie MojaFirma muszą skonfigurować zdalne klienty Windows XP, wykonując następujące czynności:

1. W menu **Start** systemu Windows XP rozwiń **Wszystkie programy → Akcesoria → Komunikacja → Kreator nowego połączenia**.
2. Na stronie Zapraszamy przeczytaj informacje ogólne. Kliknij przycisk **Dalej**.
3. Na stronie Typ połączenia sieciowego wybierz opcję **Połącz z siecią w miejscu pracy**. Kliknij przycisk **Dalej**.
4. Na stronie Połączenie sieciowe wybierz opcję **Połączenie wirtualnej sieci prywatnej**. Kliknij przycisk **Dalej**.
5. Na stronie Nazwa połączenia wpisz Połączenie z oddziałem w polu **Nazwa firmy**. Kliknij przycisk **Dalej**.
6. Na stronie Sieć publiczna wybierz opcję **Nie wybieraj początkowego połączenia**. Kliknij przycisk **Dalej**.
7. Na stronie Wybór serwera sieci VPN wpisz 192.168.1.2 (2001:DB8::2 w IPv6) w polu **Nazwa hosta lub adres IP**. Kliknij przycisk **Dalej**.
8. Na stronie Dostępność połączenia wybierz opcję **Tylko do mojego użytku**. Kliknij przycisk **Dalej**.
9. Na stronie Podsumowanie kliknij opcję **Dodaj skrót do tego połączenia na moim pulpicie**. Kliknij przycisk **Zakończ**.
10. Kliknij ikonę **Połącz z MojaFirma** utworzoną na pulpicie.
11. Na stronie Połączenie z MojaFirma wpisz nazwę użytkownika i hasło podane przez administratora.
12. Wybierz opcję **Zapisz tę nazwę użytkownika i hasło dla następujących użytkowników** oraz **Tylko ja**. Kliknij **Właściwości**.
13. Na stronie **Zabezpieczenia** sprawdź, czy wybrane są następujące **Opcje zabezpieczeń**:
    - **Typowe**
    - **Wymagaj bezpiecznego hasła**
    - **Wymagaj szyfrowania danych**

    Kliknij opcję **Ustawienia protokołu IPSec**.
14. Na stronie Ustawienia protokołu IPSec wybierz opcję **Użyj wstępnego klucza współużytkowanego do uwierzytelnienia** i w polu **Wstępny klucz współużytkowany** wpisz kluczmojejfirmy. Kliknij przycisk **OK**.
15. Na stronie Sieć jako **Typ sieci VPN** wybierz opcję **Sieć VPN z protokołem L2TP i IPSec**. Kliknij przycisk **OK**.
16. Zaloguj się za pomocą nazwy użytkownika i hasła, a następnie kliknij przycisk **Połącz**.

Aby uruchomić połączenie VPN po stronie klienta, kliknij ikonę wyświetloną na pulpicie po zakończeniu pracy kreatora połączenia.

Testowanie połączenia VPN między punktami końcowymi

Po zakończeniu konfigurowania połączenia między systemem A a zdalnymi użytkownikami i pomyślnym uruchomieniu połączenia należy przetestować połączenia, aby upewnić się, że zdalne hosty mogą się ze sobą komunikować.

Aby przetestować połączenia, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń ***System A*** → **Sieć**.
2. Kliknij prawym przyciskiem myszy opcję **Konfiguracja TCP/IP** i wybierz **Narzędzia**, a następnie wybierz opcję **Ping**.
3. W oknie dialogowym **Ping z** wpisz w polu **Ping** wartość 10.1.1.101 (2001:DA8::1:101 w przypadku IPv6).

   Uwaga: 10.1.1.101 oznacza adres IP przypisany dynamicznie (do zdalnego klienta sprzedaży) z puli adresów podanej w profilu terminatora L2TP w systemie A.
4. Kliknij przycisk **Wykonaj ping**, aby sprawdzić połączenie z systemu A do zdalnej stacji roboczej. Kliknij przycisk **OK**.

Aby przetestować połączenie z klienta zdalnego, zdalny pracownik powinien wykonać następujące czynności na stacji roboczej z systemem Windows:

1. W wierszu komend wpisz ping 10.1.1.2 (ping 2001:DA8::2 w przypadku IPv6). Jest to adres IP jednej ze stacji roboczych w sieci biura korporacji.
2. Powtórz te czynności, aby przetestować połączenie z biura korporacji do oddziału.

Scenariusz: używanie translacji adresów sieciowych w sieci VPN

W tym scenariuszu firma zamierza wymieniać newralgiczne dane z jednym z partnerów biznesowych za pomocą sieci VPN. W celu dodatkowego zabezpieczenia struktury sieciowej firmy, wykorzystywana ma być translacja NAT w sieci VPN, aby ukryć przed aplikacjami, do których mają dostęp partnerzy, prywatny adres IP serwera używanego w roli hosta tych aplikacji.

Sytuacja

W tym scenariuszu za przykład posłuży sieć niewielkiej firmy produkcyjnej ze Szczecina. Jeden z kontrahentów tej firmy, dostawca podzespołów z Poznania, chce wykorzystać Internet do współpracy z tą firmą. Dla firmy produkcyjnej ogromne znacznie 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 systemu będącego hostem aplikacji, do których dostęp ma dostawca.

Połączenie VPN może służyć nie tylko do utworzenia definicji połączenia w bramie VPN w sieci firmy, 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

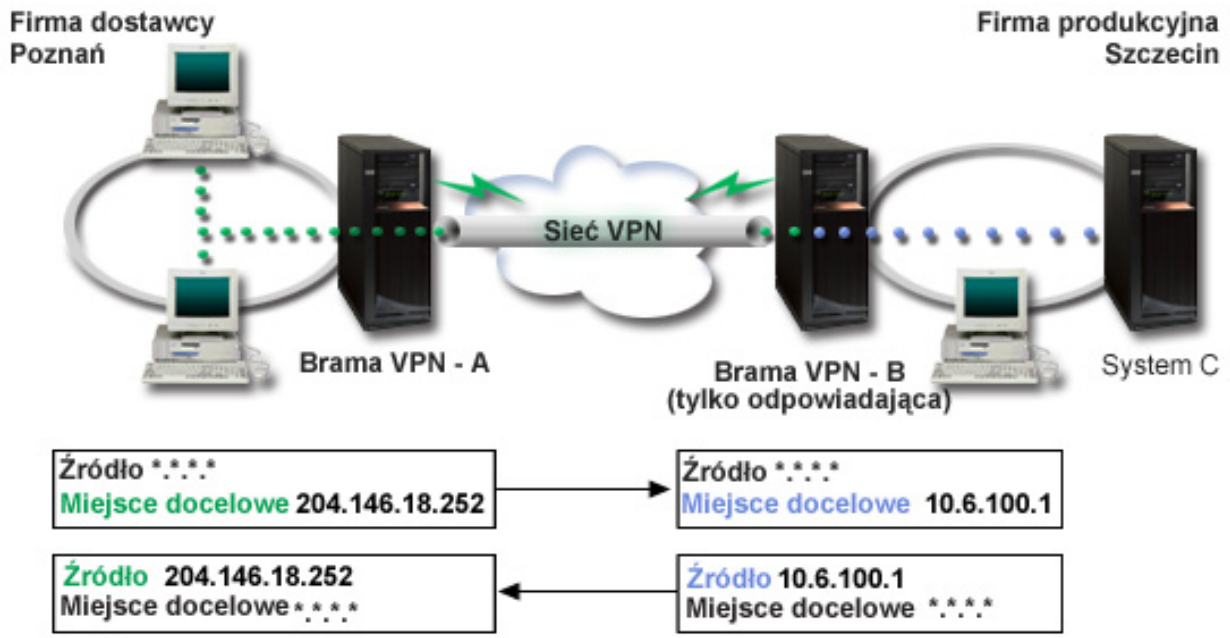
Cele tego scenariusza to:

- umożliwienie wszystkim klientom w sieci dostawcy dostępu do jednego systemu hosta w sieci producenta przez połączenie VPN między bramami,

- ukrycie prywatnego adresu IP systemu hosta w sieci producenta poprzez jego translację na publiczny adres IP za pomocą funkcji translacji adresów sieciowych dla sieci VPN (VPN NAT).

Informacje szczegółowe

Poniższy schemat przedstawia parametry sieciowe sieci dostawcy i sieci producenta:



- Brama VPN A jest skonfigurowana tak, że to zawsze ona inicjuje połączenia z bramą VPN B.
- Brama VPN A definiuje docelowy punkt końcowy połączenia jako 204.146.18.252 (adres publiczny przypisany do systemu C).
- System C ma w sieci producenta prywatny adres IP 10.6.100.1.
- Publiczny adres 204.146.18.252 został zdefiniowany w lokalnej puli usług na bramie VPN B dla prywatnego adresu systemu C - 10.6.100.1.
- Dla datagramów przychodzących brama VPN B tłumaczy adres publiczny systemu C na adres prywatny 10.6.100.1. Dla powracających datagramów wychodzących brama VPN B tłumaczy adres 10.6.100.1 z powrotem na publiczny adres systemu C - 204.146.18.252. Dla klientów w sieci dostawcy system C ma adres IP 204.146.18.252. Nigdy nie dowiedzą się oni o translacji tego adresu.

Zadania konfiguracyjne

Aby skonfigurować połączenie opisane w tym scenariuszu, należy wykonać wszystkie poniższe zadania:

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 **systemu C** za publicznym identyfikatorem 204.146.18.252.
3. Skonfiguruj na **Bramie VPN B** translację lokalnego adresu, używając adresów z lokalnej puli usług.

Pojęcia pokrewne

“Translacja adresów sieciowych dla sieci VPN” na stronie 8
Sieć VPN udostępnia możliwość translacji adresów sieciowych określanej jako translacja 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.

Planowanie sieci VPN

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.

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
- Określenie typu tworzonej sieci VPN
- Używanie doradcy podczas planowania sieci VPN

  Doradca w zakresie planowania zadaje użytkownikowi pytania dotyczące danej sieci i na podstawie udzielonych odpowiedzi przedstawia sugestie dotyczące tworzenia sieci VPN.

  Uwaga: Z doradcy w zakresie planowania sieci VPN można korzystać tylko dla połączeń, które obsługują protokół IKE (Internet Key Exchange). Dla połączeń ręcznych należy skorzystać z arkusza roboczego planowania.
- Arkusze planowania VPN

Po opracowaniu planu sieci VPN można przystąpić do jej konfigurowania.

Zadania pokrewne

Używanie doradcy podczas planowania sieci VPN

“Konfigurowanie sieci VPN” na stronie 48
W interfejsie VPN dostępnych jest kilka różnych sposobów konfigurowania połączeń VPN. Można skonfigurować połączenie ręczne lub dynamiczne.

Wymagania konfiguracyjne VPN

Aby połączenie VPN działało poprawnie w tych systemach i z klientami sieciowymi, muszą być spełnione minimalne wymagania.

Poniżej wymieniono minimalne wymagania, których spełnienie jest niezbędne do skonfigurowania połączenia VPN:

Wymagania systemowe

- System operacyjny i5/OS wersja 5 wydanie 3 lub nowszy
- Digital Certificate Manager
- System i Access for Windows
- System i Navigator
  - Komponent sieciowy System i 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 poprawnie podłączona do systemu i skonfigurowana do użycia protokołu TCP/IP
- Procesor o częstotliwości 233 MHz
- 32 MB pamięci RAM dla klientów systemu dla Windows 95.
- 64 MB pamięci RAM dla klientów systemu Windows NT 4.0 oraz Windows 2000
- System i Access for Windows oraz System i 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.

Zadania pokrewne

“Rozwiązywanie problemów z siecią VPN - pierwsze kroki” na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

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.

Na przykład, czy punkty końcowe *połączenia* różnią się 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:

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.

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.

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

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.

Wypełnianie arkuszy roboczych planowania sieci VPN

Arkusze robocze planowania sieci VPN służą do zbierania szczegółowych informacji o planach wykorzystania sieci VPN. Aby odpowiednio zaplanować strategię sieci VPN, należy wypełnić te arkusze. Mogą one także posłużyć do konfigurowania połączeń VPN.

Arkusze robocze planowania sieci VPN można także wydrukować i wypełnić w celu zebrania szczegółowych informacji o planach użycia sieci VPN.

Wybierz odpowiedni arkusz dla typu połączenia, które chcesz utworzyć.

- Arkusz roboczy planowania połączeń dynamicznych
- Arkusz roboczy planowania połączeń ręcznych
- Doradca w zakresie planowania połączeń 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 dotyczące tworzenia sieci VPN.

  Uwaga: Z doradcy w zakresie planowania sieci VPN można korzystać tylko dla połączeń dynamicznych. Dla połączeń ręcznych należy skorzystać z arkusza roboczego planowania.

Jeśli użytkownik ma zamiar tworzyć wiele połączeń o podobnych właściwościach, może ustawić wartości domyślne dla sieci 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**.

Informacje pokrewne

Doradca w zakresie planowania połączeń VPN

Arkusz roboczy planowania połączeń dynamicznych

Należy wypełnić ten arkusz roboczy przed skonfigurowaniem połączenia dynamicznego.

Należy wypełnić ten arkusz roboczy przed utworzeniem dynamicznych połączeń VPN. W arkuszu założono, że będzie używany Kreator nowego połączenia. Kreator ten umożliwia skonfigurowanie VPN na podstawie podstawowych wymagań w zakresie ochrony. W niektórych przypadkach może być konieczne dostosowanie właściwości, jakie kreator konfiguruje dla połączenia. Na przykład można zdecydować, że wymagane jest kronikowanie lub uruchamianie serwera VPN każdorazowo po uruchomieniu 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.

Tabela 9. Wymagania systemowe

Lista kontrolna wymagań wstępnych	**Odpowiedzi**
Czy używany system operacyjny to i5/OS w wersji V5R3 lub nowszej?	Tak
Czy opcja Digital Certificate Manager jest zainstalowana?	Tak
Czy zainstalowano program System i Access for Windows?	Tak
Czy zainstalowano program System i Navigator?	Tak
Czy zainstalowano składnik Sieć programu System i Navigator?	Tak
Czy zainstalowano program IBM TCP/IP Connectivity Utilities for i5/OS?	Tak
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	Tak
Czy w systemie 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

Tabela 9. Wymagania systemowe (kontynuacja)

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

Tabela 10. Konfiguracja VPN

Informacje potrzebne do skonfigurowania dynamicznego połączenia VPN	**Odpowiedzi**
Jakiego typu połączenie jest tworzone? • Między bramami • Między hostem i bramą • Między bramą i hostem • Między hostami	
Jaka nazwa zostanie nadana grupie z kluczem dynamicznym?	
Jakiego typu ochrony i wydajności systemu wymaga się do zabezpieczenia kluczy? • Najwyższa ochrona, najniższa wydajność • Zrównoważenie ochrony i wydajności • Najniższa ochrona i najwyższa wydajność	
Czy do uwierzytelnienia połączenia używane są certyfikaty? Jeśli nie, jaki jest wstępny klucz współużytkowany?	
Jaki jest identyfikator lokalnego serwera kluczy?	
Jaki jest identyfikator lokalnego serwera kluczy?	
Jaki jest identyfikator zdalnego serwera kluczy?	
Jaki jest identyfikator zdalnego punktu końcowego danych?	
Jakiego typu ochrony i wydajności systemu wymaga się do zabezpieczenia danych? • Najwyższa ochrona, najniższa wydajność • Zrównoważenie ochrony i wydajności • Najniższa ochrona i najwyższa wydajność	

Arkusz roboczy planowania połączeń ręcznych

Należy wypełnić ten arkusz roboczy przed skonfigurowaniem połączenia ręcznego.

Arkusz roboczy ułatwia tworzenie połączeń sieci VPN (Virtual Private Network), które nie używają protokołu IKE do zarządzania kluczami. Przed przystąpieniem do konfigurowania połączeń VPN należy odpowiedzieć na wszystkie pytania w poniższym formularzu:

Tabela 11. Wymagania systemowe

Lista kontrolna wymagań wstępnych	**Odpowiedzi**
Czy w systemie działa system operacyjny i5/OS w wersji V5R3 lub nowszej?	
Czy zainstalowano program Digital Certificate Manager?	
Czy zainstalowano program System i Access for Windows?	
Czy zainstalowano program System i Navigator?	
Czy zainstalowano składnik Sieć programu System i Navigator?	
Czy zainstalowano program IBM TCP/IP Connectivity Utilities for i5/OS?	
Czy wartość systemowa zachowania danych ochrony serwera (QRETSVRSEC *SEC) wynosi 1?	

Tabela 11. Wymagania systemowe (kontynuacja)

Czy w systemie 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 AH i ESP?	
Czy konfiguracja firewalli umożliwia przekazywanie IP?	

Tabela 12. Konfiguracja VPN

Informacje potrzebne do skonfigurowania ręcznych połączeń VPN	**Odpowiedzi**
Jakiego typu połączenie jest tworzone? • Między hostami • Między hostem i bramą • Między bramą i hostem • Między bramami	
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 połączeń VPN.	
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 Protokół IP Security (IPSec).	
Z jakiego algorytmu uwierzytelniania będzie korzystało połączenie (HMAC-MD5 lub HMAC-SHA)?	
Z jakiego algorytmu szyfrowania będzie korzystało połączenie (DES-CBC lub 3DES-CBC)? **Uwaga:** Algorytm szyfrowania należy określić tylko wtedy, gdy jako protokół IPSec określono protokół ESP.	
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. Klucz przychodzący musi dokładnie odpowiadać kluczowi wychodzącemu zdalnego serwera.	
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. Klucz wychodzący musi dokładnie odpowiadać kluczowi przychodzącemu zdalnego serwera.	
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. Klucz przychodzący musi dokładnie odpowiadać kluczowi wychodzącemu zdalnego serwera.	

Tabela 12. Konfiguracja VPN (kontynuacja)

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. Klucz wychodzący musi dokładnie odpowiadać kluczowi przychodzącemu zdalnego serwera.	
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. Przychodzący indeks SPI musi dokładnie odpowiadać wychodzącemu indeksowi SPI zdalnego serwera.	
Jaki jest wychodzący indeks SPI? Wychodzący indeks SPI jest 4-bajtowym łańcuchem szesnastkowym. Wychodzący indeks SPI musi dokładnie odpowiadać przychodzącemu indeksowi SPI zdalnego serwera.	

Pojęcia pokrewne

"Translacja adresów sieciowych dla sieci VPN" na stronie 8
Sieć VPN udostępnia możliwość translacji adresów sieciowych określanej jako translacja 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.

Konfigurowanie sieci VPN

W interfejsie VPN dostępnych jest kilka różnych sposobów konfigurowania połączeń VPN. Można skonfigurować połączenie ręczne lub dynamiczne.

Połączenie dynamiczne to takie, które dynamicznie generuje i negocjuje klucze zabezpieczające połączenie, w czasie, gdy jest ono aktywne, za pomocą protokołu IKE (Internet Key Exchange). 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 nie zapewnia obsługi negocjacji IKE, a co za tym idzie, 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 takie rozwiązanie zagraża bezpieczeństwu, można zamiast tego utworzyć połączenie dynamiczne.

Pojęcia pokrewne

"Planowanie sieci VPN" na stronie 43
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 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 konieczne jest dodanie do połączenia VPN pewnych funkcji, na przykład funkcji kronikowania lub translacji adresu sieciowego dla VPN (VPN NAT), to można dokładniej dostosować konfigurację sieci VPN za pomocą arkuszy właściwości odpowiedniej grupy z kluczem dynamicznym lub

odpowiedniego 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 sieci 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 System i Navigator rozwiń **system → 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**.

Zadania pokrewne

Doradca w zakresie planowania połączeń VPN

Konfigurowanie strategii bezpieczeństwa VPN

Po zaplanowaniu sposobu korzystania z połączeń VPN należy zdefiniować strategię bezpieczeństwa VPN.

Uwaga: Po skonfigurowaniu strategii bezpieczeństwa sieci VPN należy przystąpić do konfigurowania bezpiecznych połączeń.

Zadania pokrewne

"Konfigurowanie bezpiecznego połączenia VPN" na stronie 50
Po zdefiniowaniu strategii ochrony dla połączenia należy skonfigurować połączenie chronione.

Konfigurowanie strategii protokołu IKE

Strategia protokołu IKE (Internet Key Exchange) definiuje poziom ochrony uwierzytelniania i szyfrowania używany przez protokół IKE podczas negocjacji w fazie 1.

Podczas fazy 1. negocjacji IKE określane są klucze, które zabezpieczają wiadomości przesyłane następnie w fazie 2. negocjacji. W wypadku 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.

Do uwierzytelnienia fazy 1. negocjacji w połączeniu VPN używany jest albo podpis RSA, albo wstępne klucze współużytkowane. Jeśli planowane jest użycie certyfikatów cyfrowych do uwierzytelniania serwerów kluczy, to należy najpierw je skonfigurować za pomocą programu Digital Certificate Manager. 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 System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Strategie bezpieczeństwa IP** (System > Network > IP Policies > Virtual Private Networking > IP Security Policies).
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**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

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 uzgadniania, należy wybrać trudne hasła, których nie można złamać podczas ataku ze słownikiem. Zaleca się również okresowe zmiany haseł. Aby przy wymianie kluczy wymusić użycie trybu głównego uzgadniania, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Wybierz **Virtual Private Networking → Strategie bezpieczeństwa IP → Strategie protokołu Internet Key Exchange**, aby wyświetlić obecnie zdefiniowane strategie wymiany klucza w prawym panelu.
3. Kliknij prawym przyciskiem myszy daną strategię wymiany klucza i wybierz opcję **Właściwości**.
4. Na stronie Transformacje wybierz **Strategia odpowiadania**. Pojawi się okno dialogowe Strategia odpowiadania IKE.
5. W polu Ochrona tożsamości, anuluj wybór **Agresywny tryb uzgadniania IKE (bez ochrony tożsamości)**.
6. Kliknij przycisk **OK**, aby wrócić do okna dialogowego Właściwości.
7. Kliknij przycisk **OK** ponownie, aby zapisać zmiany.

Uwaga: Ustawienie pola ochrony tożsamości odnosi się do każdej wymiany ze zdalnym serwerem kluczy, gdyż istnieje tylko jedna odpowiadająca całemu systemowi strategia IKE. Główny tryb uzgadniania gwarantuje, że system inicjujący może żądać tylko strategii wymiany kluczy trybu głównego.

Pojęcia pokrewne

"Zarządzanie kluczami" na stronie 6
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.

Zadania pokrewne

Program Digital Certificate Manager

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 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.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Strategie bezpieczeństwa IP** (System > Network > IP Policies > Virtual Private Networking > IP Security Policies).
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**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

Pojęcia pokrewne

"Zarządzanie kluczami" na stronie 6
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.

Konfigurowanie bezpiecznego 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 należeć będą 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 strategie, 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 zadania przedstawione w części 1 i części 2:

Pojęcia pokrewne

"Konfigurowanie strategii bezpieczeństwa VPN" na stronie 49
Po zaplanowaniu sposobu korzystania z połączeń VPN należy zdefiniować strategię bezpieczeństwa VPN.

"Konfigurowanie reguł pakietów VPN" na stronie 52
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.

Zadania pokrewne

"Aktywowanie reguł pakietów VPN" na stronie 56
Aby można było uruchomić połączenie VPN, należy najpierw aktywować reguły pakietów VPN.

Część 1: Konfigurowanie grupy z kluczem dynamicznym

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
2. Kliknij prawym przyciskiem myszy opcję **Według grupy** i wybierz opcję **Nowa grupa z kluczem dynamicznym**.
3. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

Część 2: Konfigurowanie połączenia z kluczem dynamicznym

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia → Według grupy**.
2. W lewym panelu okna programu System i Navigator kliknij prawym przyciskiem myszy grupę z kluczem dynamicznym utworzoną w części 1 i wybierz opcję **Nowe połączenie z kluczem dynamicznym**.
3. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

Po wykonaniu tych czynności należy aktywować reguły pakietów wymagane przez połączenie do prawidłowego działania.

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

Konfigurowanie połączenia ręcznego

Połączenie ręczne to takie, w którym trzeba skonfigurować wszystkie właściwości sieci VPN bez użycia kreatorów.

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 stanowi to zagrożenie bezpieczeństwa, a oba punkty końcowe połączenia obsługują protokół IKE, to można rozważyć skonfigurowanie połączenia dynamicznego.

Aby zdefiniować właściwości połączenia ręcznego, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → → Bezpieczne połączenia**.
2. Prawym przyciskiem myszy kliknij pozycję **Wszystkie połączenia** i wybierz opcję **Nowe połączenie ręczne**.
3. Wypełnij wszystkie arkusze właściwości. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

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

Zadania pokrewne

"Konfigurowanie reguły filtrowania strategii" na stronie 54
Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguły filtrowania strategii przez VPN.

Konfigurowanie połączenia dynamicznego

Połączenie dynamiczne to takie, które dynamicznie generuje i negocjuje klucze zabezpieczające połączenie, w czasie, gdy jest ono aktywne, za pomocą protokołu IKE (Internet Key Exchange).

Aby skonfigurować połączenie dynamiczne, należy w kreatorze nowego połączenia z kluczem dynamicznym wykonać następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia → Według grupy**.
2. Kliknij prawym przyciskiem myszy konkretną grupę z kluczem dynamicznym i wybierz opcję **Nowe połączenie z kluczem dynamicznym** (New Dynamic-Key Connection).
3. Wypełnij wszystkie arkusze właściwości. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Kliknij przycisk **OK**, aby zapisać zmiany.

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 System i 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 System i Navigator. Aby uzyskać informacje na temat innych opcji połączeń VPN i filtrowania, zapoznaj się z sekcją VPN i filtrowanie IP 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. Może pojawić się potrzeba dodania innych reguł Pre-IPSec w zależności od określonego środowiska sieciowego i strategii bezpieczeństwa.

  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 niejawny.
- Konfigurowanie reguły filtrowania strategii

  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 ruch, który wcześniej działał, w tajemniczy sposób przestał działać po aktywowaniu 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 zdefiniować interfejs, do którego będą one stosowane, a następnie aktywować je.

Poprawne skonfigurowanie reguł filtrowania ma zasadnicze znaczenie. W przeciwnym razie mogą one zablokować cały ruch IP przychodzący do systemu i wychodzący z niego. Dotyczy to również połączenia z programem System i Navigator używanym do konfigurowania reguł filtrowania.

Jeśli reguły filtrowania nie zezwalają na ruch związany z serwerem System i, to System i Navigator nie może komunikować się z systemem. Jeśli zaistnieje taka sytuacja, jedynym wyjściem będzie zalogowanie się do systemu przy użyciu interfejsu, który w dalszym ciągu umożliwia łączność, na przykład poprzez konsolę Operations Console. 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 aktywować.

Pojęcia pokrewne

“Sieci VPN i filtrowanie IP” na stronie 11
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 pojęciach dotyczących filtrowania związanych z sieciami VPN.

Zadania pokrewne

“Konfigurowanie bezpiecznego połączenia VPN” na stronie 50
Po zdefiniowaniu strategii ochrony dla połączenia należy skonfigurować połączenie chronione.

Konfigurowanie reguły filtrowania typu Pre-IPSec

Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguły 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 System i Navigator rozwiń **system → 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 systemu.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz opcję **Wstaw → Filtr** (Insert > Filter).
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 poprzez połączenie jest skonfigurowanie tylko jednego filtru typu Pre-IPSec i użycie znaków zastępczych (*) w polach **Kierunek**, **Nazwa adresu źródłowego** oraz **Nazwa adresu docelowego**.

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

Zadania pokrewne

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

Konfigurowanie reguły filtrowania strategii

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 na stronie 55.

1. W programie System i Navigator rozwiń **system → 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 systemu.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz opcję **Wstaw → Filtr** (Insert > Filter).
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 zdefiniowanie interfejsu, do którego zostaną zastosowane te reguły filtrowania.

Uwaga: 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 połączenia, które wcześniej działały, w tajemniczy sposób przestały działać po aktywowaniu reguł pakietów VPN. Aby umożliwić przesyłanie danym interfejsem ruchu innego niż VPN, należy dodać dla tego ruchu jawną regułę PERMIT.

Zadania pokrewne

"Konfigurowanie połączenia ręcznego" na stronie 52
Połączenie ręczne to takie, w którym trzeba skonfigurować wszystkie właściwości sieci VPN bez użycia kreatorów.

"Konfigurowanie reguły filtrowania typu Pre-IPSec" na stronie 53
Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguły filtrowania strategii przez VPN.

"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.

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, interfejs Reguły pakietów będzie w dalszym ciągu otwarty. W takim wypadku należy przejść do etapu 4.

1. W programie System i Navigator rozwiń **system → 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 systemu.
3. W oknie Powitanie wybierz opcję **Utwórz nowy plik reguł pakietów** i kliknij przycisk **OK**.
4. W Edytorze reguł pakietów wybierz opcję **Wstaw → Interfejs filtru** (Insert > Filter Interface).
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 dodać nazwę każdego zestawu dla skonfigurowanych filtrów.
8. Kliknij przycisk **OK**.
9. Zapisz plik reguł. Plik zostanie zapisany w zintegrowanym systemie plików z rozszerzeniem .i3p.

   Uwaga: Nie zapisuj 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 filtrowania, należy aktywować je przed uruchomieniem połączenia VPN.

Zadania pokrewne

“Konfigurowanie reguły filtrowania strategii” na stronie 54
Zadanie to należy wykonać tylko wtedy, gdy nie zdecydowano się na automatyczne generowanie reguły filtrowania strategii przez VPN.

“Aktywowanie reguł pakietów VPN”
Aby można było uruchomić połączenie VPN, należy najpierw aktywować reguły pakietów VPN.

Aktywowanie reguł pakietów VPN

Aby można było uruchomić połączenie VPN, należy najpierw aktywować reguły pakietów VPN.

Jeśli w systemie są uruchomione połączenia VPN, nie można aktywować (ani dezaktywować) reguł pakietów. Dlatego przed aktywowaniem 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 aktywowanie 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 aktywowane za pomocą Edytora reguł pakietów, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Reguły pakietów** (Packet Rules) i wybierz opcję **Aktywuj** (Activate). Spowoduje to otwarcie okna dialogowego **Aktywuj reguły pakietów** (Activate Packet Rules).
3. Wybierz aktywowanie 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 aktywować 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 aktywowania 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 aktywowaniu reguł filtrowania można uruchomić połączenie VPN.

Zadania pokrewne

"Konfigurowanie bezpiecznego połączenia VPN" na stronie 50
Po zdefiniowaniu strategii ochrony dla połączenia należy skonfigurować połączenie chronione.

"Definiowanie interfejsu dla reguł filtrowania VPN" na stronie 55
Po skonfigurowaniu reguł pakietów i wszelkich innych reguł potrzebnych przy połączeniu VPN należy zdefiniować interfejs, do którego zostaną one zastosowane.

"Uruchamianie połączenia VPN"
Wykonanie opisanych w tej sekcji zadań pozwoli uruchomić połączenie inicjowane lokalnie.

Konfigurowanie poufności przepływu danych

Jeśli strategie danych są skonfigurowane dla trybu tunelowego, można użyć funkcji poufności przepływu danych (traffic flow confidentiality - TFC) w celu ukrycia faktycznej długości pakietów danych przesyłanych przez połączenie VPN.

Funkcja TFC dopełnia przesyłane pakiety pakietami fikcyjnymi o różnej długości przesyłanymi w losowych odstępach, co umożliwia ukrycie rzeczywistej długości pakietów. Jest to przydatne jako dodatkowy środek ochrony przed atakami polegającymi na zgadywaniu, jaki typ danych jest przesyłany na podstawie długości pakietu. Aktywowanie TFC wzmacnia ochronę kosztem wydajności systemu. Dlatego należy przetestować wydajność systemu przed i po aktywowaniu funkcji TFC dla połączenia VPN. Funkcja TFC nie jest negocjowana przez protokoły IKE. Należy aktywować funkcję TFC tylko wtedy, gdy obydwa systemy umożliwiają jej obsługę.

Aby aktywować funkcję TFC dla połączenia VPN, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń serwer **> Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia → Wszystkie połączenia**.
2. Kliknij prawym przyciskiem połączenie, dla którego ma być aktywowane TFC i wybierz opcję **Właściwości**.
3. Na karcie **Ogólne** wybierz opcję **Używaj TFC w trybie tunelowym**.

Konfigurowanie rozszerzonego numeru kolejnego (ESN)

Numeru ESN można używać do zwiększenia szybkości przesyłania danych przez połączenie VPN.

Jeśli wykorzystywany jest protokół AH lub protokół ESP oraz algorytm szyfrowania AES, może wystąpić zapotrzebowanie na aktywowanie numeru ESN. Umożliwia on przesyłanie dużych woluminów danych przy dużej szybkości bez ponownego szyfrowania za pomocą klucza. Połączenie VPN korzysta z 64-bitowych numerów kolejnych zamiast 32-bitowych numerów w IPSec. Używanie 64-bitowych numerów kolejnych wydłuża czas do wymiany klucza, co przeciwdziała wyczerpaniu numerów kolejnych i minimalizuje użycie zasobów systemowych.

Aby aktywować ESN dla połączenia VPN, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN**.
2. Kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz **Właściwości**.
3. Na karcie **Ogólne** wybierz opcję **Użyj numeru ESN**.

Uruchamianie połączenia VPN

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

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Jeśli serwer VPN nie jest uruchomiony, kliknij prawym przyciskiem myszy pozycję **Sieć VPN** i wybierz opcję **Uruchom**.
3. Sprawdź, czy aktywowano reguły pakietów.
4. Rozwiń **Virtual Private Networking → 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**.

Zadania pokrewne

"Aktywowanie reguł pakietów VPN" na stronie 56
Aby można było uruchomić połączenie VPN, należy najpierw aktywować reguły pakietów VPN.

"Rozwiązywanie problemów z siecią VPN - pierwsze kroki" na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

Zarządzanie siecią VPN

Interfejs VPN dostępny w programie System i Navigator umożliwia obsługę wszystkich zadań związanych z zarządzaniem siecią VPN, takich jak zatrzymywanie połączenia i wyświetlanie jego atrybutów.

Interfejs sieci VPN dostępny w programie System i Navigator umożliwia obsługę wszystkich zadań administracyjnych, takich jak:

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.

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 System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Prawym przyciskiem myszy kliknij pozycję **Sieć VPN** i wybierz opcję **Domyślne**.
3. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
4. Po wypełnieniu wszystkich arkuszy właściwości kliknij przycisk **OK**.

Resetowanie połączeń w stanie błędu

Zresetowanie połączenia po wystąpieniu błędu powoduje przełączenie go w stan bezczynności.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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 błędzie

Wykonanie tego zadania pozwala określić, dlaczego połączenie powoduje błąd.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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**.

Zadania pokrewne

“Rozwiązywanie problemów z siecią VPN - pierwsze kroki” na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

Wyświetlanie atrybutów aktywnych połączeń

W tej sekcji opisano zadania umożliwiające sprawdzenie statusu i innych atrybutów połączeń aktywnych.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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 ma być wyświetlone, a następnie wybierz opcję **Właściwości**.
4. Przejdź do strony **Bieżące atrybuty**, aby wyświetlić atrybuty połączenia.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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 wyświetlone w oknie programu System i Navigator.

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

Pojęcia pokrewne

“Często spotykane komunikaty o błędach Menedżera połączeń VPN” na stronie 73
Gdy wystąpi błąd połączenia VPN, Menedżer połączeń VPN rejestruje dwa komunikaty w protokole zadania QTOVMAN.

Wyświetlanie danych śledzenia serwera VPN

Program ten umożliwia skonfigurowanie, uruchomienie, zatrzymanie i wyświetlenie informacji o śledzeniu serwerów Menedżera połączeń VPN (VPN Connection Manager) i Menedżera kluczy VPN (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.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP**.
2. Prawym przyciskiem myszy kliknij **Virtual Private Networking**, wybierz **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 **Śledzenie sieci VPN** (Virtual Private Networking Trace) kliknij ikonę  (Opcje).
2. Na stronie **Menedżer połączeń** określ, jaki typ śledzenia ma być generowany przez serwer Menedżera połączeń.
3. Na stronie **Menedżer kluczy** określ typ śledzenia, jaki ma być uruchomiony przez serwer Menedżera kluczy.
4. Kliknij przycisk **Pomoc**, jeśli masz pytania na temat wypełniania strony lub dowolnego z pól.
5. Kliknij przycisk **OK**, aby zapisać zmiany.
6. Kliknij ikonę  (Start), aby uruchomić śledzenie. Od czasu do czasu klikaj ikonę  (Odśwież), aby wyświetlić najnowsze informacje śledzenia.

Wyświetlanie protokołów zadań serwera VPN

W tej sekcji przedstawiono instrukcje dotyczące wyświetlania protokołów zadań VPN Key Manager i Menedżera połączeń VPN.

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

1. W programie System i Navigator rozwiń **system → 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

W sekcji opisano sposób wyświetlania atrybutów powiązań Security Association (SA) przypisanych aktywnemu połączeniu.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
2. Kliknij pozycję **Wszystkie połączenia**, aby wyświetlić listę połączeń w prawej części okna.
3. Prawym przyciskiem myszy kliknij odpowiednie aktywne połączenie i wybierz **Powiązania bezpieczeństwa**. Spowoduje to otwarcie okna umożliwiającego wyświetlenie właściwości każdego powiązania SA przypisanego do konkretnego połączenia.

Zatrzymywanie połączenia VPN

Wykonanie opisanych w tej sekcji czynności spowoduje zatrzymanie aktywnych połączeń.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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

Przed usunięciem obiektu konfiguracyjnego VPN z bazy danych strategii należy dokładnie rozważyć wpływ, jaki to będzie miało na inne połączenia i grupy połączeń.

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

1. W programie System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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 z siecią VPN

Do rozwiązywania niektórych podstawowych problemów, jakie mogą wystąpić podczas konfigurowania połączenia VPN, należy zastosować następujące metody.

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. Ze względu na tę złożoność mogą od czasu do czasu występować problemy 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 następujących tematach znajdują się wskazówki dotyczące rozwiązywania różnych problemów, jakie mogą wystąpić podczas używania sieci VPN.

Rozwiązywanie problemów z siecią VPN - pierwsze kroki

Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

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 instalacyjne VPN.
3. Przejrzyj wszystkie komunikaty o błędach znalezione w oknie Informacje o błędach lub w protokołach zadań serwera VPN, 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 końcowego 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 filtru IP.
5. Śledzenie komunikacji w systemie to kolejne miejsce, w którym można znaleźć ogólne informacje o tym, czy system lokalny odbiera lub wysyła żądania połączenia.
6. Komenda Śledzenie aplikacji TCP/IP (Trace TCP Application - TRCTCPAPP) udostępnia następny sposób zlokalizowania problemu. Serwis IBM zazwyczaj używa komendy TRCTCPAPP do uzyskania danych wyjściowych śledzenia w celu analizy problemów dotyczących połączenia.

Pojęcia pokrewne

"Wymagania konfiguracyjne VPN" na stronie 43
Aby połączenie VPN działało poprawnie w tych systemach i z klientami sieciowymi, muszą być spełnione minimalne wymagania.

"Rozwiązywanie problemów z siecią VPN za pomocą protokołów zadań VPN" na stronie 73
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.

"Rozwiązywanie problemów z siecią VPN za pomocą funkcji śledzenia komunikacji" na stronie 78
System IBM i5/OS 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.

Zadania pokrewne

"Wyświetlanie informacji o błędzie" na stronie 59
Wykonanie tego zadania pozwala określić, dlaczego połączenie powoduje błąd.

“Rozwiązywanie problemów z siecią VPN za pomocą kroniki QIPFILTER” na stronie 68
Ta sekcja zawiera informacje dotyczące reguł filtrowania w sieci VPN.

“Uruchamianie połączenia VPN” na stronie 57
Wykonanie opisanych w tej sekcji zadań pozwoli uruchomić połączenie inicjowane lokalnie.

Sprawdzanie 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. Zacznij 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; w tym celu należy wpisać adres zdalnego systemu i użyć klawisza PF10 do wprowadzenia dodatkowych parametrów, a następnie podać 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 być routery pośredniczące w komunikacji lub zapora firewall, która filtruje pakiety IP i może filtrować pakiety 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. W celu sprawdzenia możliwości połączenia można użyć innych protokołów IP między dwoma systemami, na przykład Telnet lub FTP.
2. Sprawdź, czy reguły filtrowania dla połączenia VPN zostały aktywowane. Czy filtrowanie uruchamia się prawidłowo? Jeśli odpowiedź brzmi **tak**, przejdź do punktu 3. Jeśli **nie**, sprawdź komunikaty w oknie Reguły pakietów w programie System i Navigator. Sprawdź, czy reguły filtrowania nie włączają translacji NAT (Network Address Translation) dla ruchu VPN.
3. Uruchom połączenie VPN. Czy połączenie uruchamia się prawidłowo? Jeśli odpowiedź brzmi **tak**, przejdź do punktu 4. Jeśli **nie**, sprawdź błędy w protokołach zadań QTOVMAN i QTOKVPNIKE. Aby można było korzystać z połączeń VPN, dostawca usług internetowych (ISP) i każda brama bezpieczeństwa 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 aktywować 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

Poniższe informacje są pomocne podczas przeglądania typowych komunikatów o błędach sieci VPN i znajdowania możliwych rozwiązań.

Uwaga: Konfigurowanie połączenia VPN 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.

Komunikat o błędzie VPN: TCP5B28

Przy próbie aktywowania reguł filtrowania dla interfejsu wyświetlany jest komunikat: TCP5B28 Naruszenie kolejności definicji połączenia (CONNECTION_DEFINITION).

Objaw:

Przy próbie aktywowania reguł filtrowania dla interfejsu wyświetlany jest następujący komunikat:

```
TCP5B28: Naruszenie kolejności definicji połączenia (CONNECTION_DEFINITION)
```

Możliwe rozwiązanie:

Próbowano aktywować reguły filtrowania z definicjami połączenia, które były uporządkowane w innej kolejności niż zestaw reguł aktywowany poprzednio. Najprostszym sposobem usunięcia tego błędu jest aktywowanie reguł filtrowania dla **wszystkich interfejsów** zamiast dla konkretnego interfejsu.

Komunikat o błędzie VPN: Nie można znaleźć pozycji

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

Objaw:

Po kliknięciu prawym przyciskiem myszy obiektu w oknie VPN i wybraniu opcji **Właściwości** lub **Usuń** wyświetlony zostaje następujący komunikat:

Możliwe rozwiązanie:

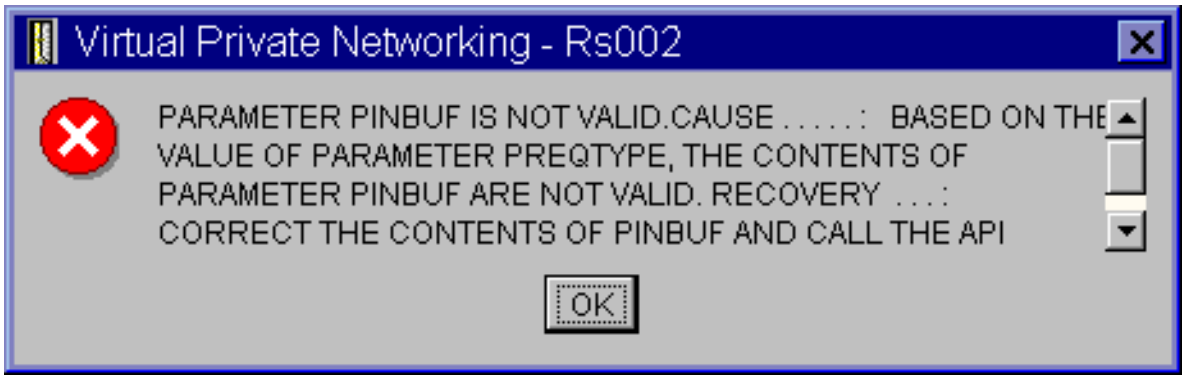
- Być może usunięto obiekt lub zmieniono jego nazwę i jeszcze nie odświeżono okna. W rezultacie obiekt jest w dalszym ciągu wyświetlany w oknie Wirtualne sieci prywatne. Aby sprawdzić, czy tak jest faktycznie, z menu **Widok** wybierz opcję **Odśwież**. Jeśli obiekt jest w dalszym ciągu wyświetlany w oknie Wirtualne sieci prywatne, przejdź do następnego punktu.
- Po skonfigurowaniu właściwości obiektu mógł wystąpić błąd komunikacji między serwerem VPN a systemem użytkownika. Wiele obiektów wyświetlanych w oknie VPN odnosi się do więcej niż jednego obiektu w bazie danych strategii VPN. Oznacza to, że w wyniku błędów komunikacji niektóre obiekty w bazie danych nadal są powiązane z obiektem w sieci VPN. 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 otwarcie 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 łączy z bazą danych strategii VPN, które zostały zerwane. Dzięki temu będzie można usunąć obiekt.

Komunikat o błędzie VPN: NIEPOPRAWNY PARAMETR PINBUF

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

Objaw:

Podczas próby uruchomienia połączenia wyświetlany jest komunikat podobny do następującego:



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 VPN: Nie można znaleźć pozycji, Zdalny serwer kluczy...

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.

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 VPN: Nie można zaktualizować obiektu

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.

Objaw:

Po wybraniu **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 VPN: Nie można zaszyfrować klucza...

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

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**.

Pojęcia pokrewne

“Błąd połączenia VPN: Wszystkie klucze są puste” na stronie 66
Podczas wyświetlania właściwości połączenia ręcznego wszystkie wstępne klucze współużytkowane i klucze algorytmów dla połączenia są puste.

Komunikat o błędzie VPN: CPF9821

Podczas próby rozwinięcia lub otwarcia kontenera Strategie IP (IP Policies) w programie System i Navigator, wyświetlany jest komunikat CPF9821 - Brak uprawnienia do programu QTFRPRS w bibliotece QSYS.

Objaw:

Podczas próby rozwinięcia kontenera Strategie IP (IP Policies) w programie System i Navigator, wyświetlany jest komunikat CPF9821 - Brak uprawnienia do programu QTFRPRS w bibliotece QSYS.

Możliwe rozwiązanie:

Być może użytkownik nie ma wymaganych uprawnień do odtwarzania bieżącego statusu reguł pakietów lub

Menedżera połączeń VPN. Należy sprawdzić posiadanie uprawnienia *IOSYSCFG, które umożliwia dostęp do funkcji reguł pakietów w programie System i Navigator.

Błąd połączenia VPN: Wszystkie klucze są puste

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

Objaw:

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

Możliwe rozwiązanie:

Sytuacja taka występuje, gdy wartość systemowa QRETSVRSEC zostaje ustawiona z powrotem na 0. Ustawienie takie powoduje usunięcie wszystkich kluczy z bazy danych strategii sieci 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 VPN: Nie można zaszyfrować kluczy.

Pojęcia pokrewne

“Komunikat o błędzie VPN: Nie można zaszyfrować klucza...” na stronie 65
Wyświetlany jest komunikat informujący, że system nie może zaszyfrować kluczy, ponieważ wartość QRETSVRSEC musi być równa 1.

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

Przy pierwszej próbie skorzystania z interfejsu Reguły pakietów w programie System i Navigator wyświetlany jest ekran wpisania się do systemu innego niż system używany w chwili obecnej.

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 umożliwia uzyskanie odpowiedniej tabeli konwersji kodu Unicode przez program System i Access for Windows. Sytuacja taka zdarza się tylko raz.

Błąd VPN: W oknie programu System i Navigator wyświetlany jest pusty status połączenia

Brak wartości dla połączenia w kolumnie **Status** w oknie programu System i Navigator.

Objaw:

Brak wartości dla połączenia w kolumnie **Status** w oknie programu System i Navigator.

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

Po zatrzymaniu połączenia jest ono nadal wyświetlane jako aktywne w oknie programu System i Navigator.

Objaw:

Po zatrzymaniu połączenia jest ono nadal wyświetlane jako aktywne w oknie programu System i Navigator.

Możliwe rozwiązanie:

Najczęstszą przyczyną takiej sytuacji jest nieodświeżenie okna programu System i 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

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

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 (5722-AC2), a nie Cryptographic Access Provider (5722-AC3). Cryptographic Access Provider (5722-AC2) obsługuje tylko algorytm szyfrowania Data Encryption Standard (DES), ze względu na ograniczenie długości kluczy. Aby umożliwić szyfrowanie danych w systemach i5/OS V5R4 lub nowszych, nie jest już potrzebny program Cryptographic Access Provider (5722-AC2) ani (5722-AC3).

Błąd VPN: W oknie programu System i Navigator wyświetlone zostały nieoczekiwane kolumny.

Skonfigurowane zostały kolumny do wyświetlenia w oknie programu System i Navigator dla połączeń VPN; następnie, przy ponownym sprawdzeniu wyświetlane są inne kolumny.

Objaw:

Skonfigurowano kolumny do wyświetlenia w oknie programu System i Navigator dla połączeń VPN; następnie przy ponownym sprawdzeniu zostają wyświetlone 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

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

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

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.

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 **Ogóle** 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 z siecią VPN za pomocą kroniki QIPFILTER

Ta sekcja zawiera informacje dotyczące reguł filtrowania w sieci VPN.

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.

Zadania pokrewne

"Rozwiązywanie problemów z siecią VPN - pierwsze kroki" na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

Włączanie kroniki QIPFILTER

Do aktywowania kroniki QIPFILTER służy Edytor reguł pakietów w programie System i Navigator.

Funkcje protokołowania trzeba włączyć dla każdej indywidualnej reguły filtrowania. Nie ma funkcji umożliwiającej protokołowanie dla wszystkich przychodzących lub wychodzących datagramów IP.

Uwaga: Aby włączyć kronikę QIPFILTER, należy najpierw dezaktywować filtry.

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

1. W programie System i Navigator rozwiń **system → 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 aktywuj go.

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

Korzystanie z kroniki QIPFILTER

System i5/OS automatycznie tworzy kronikę przy pierwszej próbie aktywowania 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)) ENTTYP((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.

Pojęcia pokrewne

"Pola kroniki QIPFILTER"
Poniższa tabela zawiera opis pól w zbiorze wyjściowym QIPFILTER.

Pola kroniki QIPFILTER

Poniższa tabela zawiera opis pól w zbiorze wyjściowym 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)

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

Zadania pokrewne

“Korzystanie z kroniki QIPFILTER” na stronie 68
System i5/OS automatycznie tworzy kronikę przy pierwszej próbie aktywowania filtrowania pakietów IP.

Rozwiązywanie problemów z siecią VPN za pomocą kroniki QVPN

W tej sekcji przedstawiono informacje o ruchu IP i połączeniach.

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.

Włączanie kroniki QVPN

Aby włączyć kronikę VPN, należy użyć interfejsu sieci VPN w programie System i 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 System i Navigator rozwiń **system → Sieć → Strategie IP → Sieć VPN → Bezpieczne połączenia**.
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.

Wszystkie
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 aktywować 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)) ENTTYP((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/QATOVSOF do biblioteki użytkownika. Można to zrobić, korzystając z komendy Tworzenie duplikatu obiektu (Create Duplicate Object - CRTDUPOBJ). Poniżej przedstawiono przykład zastosowania komendy CRTDUPOBJ:
   ```
   CRTDUPOBJ OBJ(QATOVSOF) 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.

Pojęcia pokrewne

"Pola kroniki QVPN"
Poniższa tabela zawiera opis pól w zbiorze wyjściowym QVPN.

Pola kroniki QVPN

Poniższa tabela zawiera opis pól w zbiorze wyjściowym 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	

Nazwa pola	Długość pola	Liczbowe	Opis	Komentarze
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	
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	

Zadania pokrewne

“Korzystanie z kroniki QVPN” na stronie 71
Aby wyświetlić szczegóły dla danej pozycji w kronice QVPN, można wyświetlić pozycje kroniki na ekranie lub użyć zbioru wyjściowego.

Rozwiązywanie problemów z siecią 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.

Ważne jest, aby przeanalizować protokoły zadań po obu stronach połączenia, jeśli obie strony są serwerami System i. Kiedy nie można uruchomić połączenia dynamicznego, dobrze jest wiedzieć, co się dzieje w zdalnym systemie.

Zadania VPN, QTOVMAN i QTOKVPNIKE działają w podsystemie QSYSWRK. Można wyświetlać odpowiednie protokoły zadań za pomocą programu System i 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 komunikaty 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.

Zadania pokrewne

“Rozwiązywanie problemów z siecią VPN - pierwsze kroki” na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

Często spotykane komunikaty o błędach Menedżera połączeń VPN

Gdy wystąpi błąd połączenia VPN, Menedżer połączeń VPN rejestruje dwa komunikaty w protokole zadania QTOVMAN.

Pierwszy komunikat zawiera szczegóły dotyczące błędu. Informacje na temat tych błędów można wyświetlić w programie System i Navigator 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	Odzyskiwanie
TCP8601 Nie można uruchomić połączenia VPN [*nazwa połączenia*]	Nie można uruchomić tego połączenia VPN w związku z wystąpieniem jednego z poniższych kodów przyczyny: *0* - Poprzedni komunikat w protokole zadania 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.	1. Sprawdź dodatkowe komunikaty o błędach w protokołach zadań. 2. Usuń błędy i spróbuj ponowić żądanie. 3. Użyj programu System i Navigator do wyświetlenia statusu połączenia. Połączenia, których nie udało się uruchomić, będą w stanie błędu.
TCP8602 Wystąpił błąd podczas zatrzymywania połączenia VPN [*nazwa połączenia*]	Zażądano zatrzymania wymienionego połączenia VPN, jednak nie zatrzymało się ono lub zatrzymało wskutek błędu z kodem przyczyny: *0* - Poprzedni komunikat w protokole zadania 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.	1. Sprawdź dodatkowe komunikaty o błędach w protokołach zadań. 2. Usuń błędy i spróbuj ponowić żądanie. 3. Użyj programu System i Navigator do wyświetlenia statusu połączenia. Połączenia, których nie udało się uruchomić, będą w stanie błędu.
TCP8604 Uruchomienie połączenia VPN [*nazwa połączenia*] nie powiodło się	Uruchomienie tego połączenia VPN nie powiodło się ze względu na jeden z poniższych kodów przyczyny: *1* - Nie można dokonać translacji nazwy hosta zdalnego 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.	1. Sprawdź dodatkowe komunikaty o błędach w protokołach zadań. 2. Usuń błędy i spróbuj ponowić żądanie. 3. Użyj programu System i Navigator, aby sprawdzić lub poprawić konfigurację strategii VPN. Sprawdź, czy w grupie z kluczem dynamicznym powiązanej z tym połączeniem skonfigurowano dopuszczalne wartości.

Komunikaty o błędach Menedżera połączeń VPN

Komunikat	Przyczyna	Odzyskiwanie
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 protokołach zadań. 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 VPN.
TCP8606 VPN Key Manager nie mógł ustanowić żądanego powiązania ochronnego dla połączenia, [*nazwa połączenia*]	VPN Key Manager nie mógł ustanowić żądanego powiązania ochronnego z powodu jednego z poniższych kodów przyczyny: *24* - Uwierzytelnienie połączenia 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.	1. Sprawdź dodatkowe komunikaty o błędach w protokołach zadań. 2. Usuń błędy i spróbuj ponowić żądanie. 3. Użyj programu System i Navigator, aby sprawdzić lub poprawić konfigurację 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	Ta grupa z kluczem dynamicznym lub połączenie danych określa, że translacja adresu sieciowego (NAT) ma być wykonywana dla jednego lub większej ilości adresów, co nie powiodło się z powodu wystąpienia jednego z poniższych kodów przyczyny: *1* - Adres, do którego ma być zastosowana translacja NAT, nie jest pojedynczym adresem NAT. *2* - wszystkie dostępne adresy zostały użyte.	1. Sprawdź dodatkowe komunikaty o błędach w protokołach zadań. 2. Usuń błędy i spróbuj ponowić żądanie. 3. Użyj programu System i Navigator, aby sprawdzić lub poprawić strategię 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 protokołach zadań 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.

Komunikaty o błędach Menedżera połączeń VPN

Komunikat	Przyczyna	Odzyskiwanie
TCP8621 Lokalny punkt końcowy danych jest niedostępny	Nie można włączyć tego połączenia VPN, ponieważ lokalny punkt końcowy danych jest niedostępny.	1. Sprawdź w protokołach zadań 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 bezpieczeństwa.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. Użyj programu System i Navigator, aby zmienić strategię VPN powiązaną 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 protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. Użyj programu System i Navigator, aby wyświetlić wszystkie aktywowane połączenia, których lokalne punkty końcowe danych i zdalne punkty końcowe danych pokrywają się z połączeniem. Jeśli potrzebne są obydwa 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 protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. W programie System i Navigator wyświetl ograniczenia punktu końcowego danych dla 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.

Komunikaty o błędach Menedżera połączeń VPN

Komunikat	Przyczyna	Odzyskiwanie
TCP8625 Sprawdzanie algorytmu ESP przez połączenie VPN nie powiodło się	Nie można włączyć tego połączenia VPN, ponieważ klucz tajny powiązany z połączeniem jest niewystarczający.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. W programie System i Navigator wyświetl strategię powiązaną z tym połączeniem i wpisz inny klucz tajny. 3. Usuń wszelkie błędy i spróbuj ponowić żądanie.
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.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. W programie System i Navigator wyświetl ograniczenia punktu końcowego danych dla 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.
TCP8628 Nie załadowano reguły filtrowania połączenia	Reguła filtrowania strategii dla tego połączenia jest nieaktywna.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. W programie System i Navigator wyświetl aktywne filtry strategii. Sprawdź regułę filtrowania strategii dla tego połączenia. 3. Usuń wszelkie błędy i spróbuj ponowić żądanie.
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.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. W programie System i Navigator zwiększ liczbę adresów NAT przypisanych do tego połączenia VPN. 3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

Komunikaty o błędach Menedżera połączeń VPN

Komunikat	Przyczyna	Odzyskiwanie
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.	1. Sprawdź w protokołach zadań dodatkowe komunikaty dotyczące tego połączenia. 2. Sprawdź protokół zadania powiązany z połączeniem PPP. 3. Usuń wszelkie błędy i spróbuj ponowić żądanie.

Zadania pokrewne

“Wyświetlanie atrybutów aktywnych połączeń” na stronie 59
W tej sekcji opisano zadania umożliwiające sprawdzenie statusu i innych atrybutów połączeń aktywnych.

Rozwiązywanie problemów z siecią VPN za pomocą funkcji śledzenia komunikacji

System IBM i5/OS 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 w przypadku użycia w komendzie STRCMNTRC wielkości buforu większej niż wielkość zdefiniowana w narzędziach SST może pojawić się 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 zapełnieniu 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. Jeśli nastąpi zawinięcie zapisu śledzenia, mogą zostać utracone ważne informacje. 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(TRNLINE) 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(TRNLINE) 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 wyświetlać żądań protokołu ARP (Address Resolution Protocol), należy ustawić wartość *NO; w przeciwnym razie może pojawić się duża liczba komunikatów rozgłaszanych.

Zadania pokrewne

“Rozwiązywanie problemów z siecią VPN - pierwsze kroki” na stronie 61
Aby zapoznać się z różnymi metodami diagnozowania problemów z siecią VPN, jakie występują w systemie, należy wykonać poniższe zadania.

Informacje pokrewne dla sieci VPN

Informacje związane z kolekcją tematów dotyczących sieci VPN znajdują się w dokumentacji technicznej IBM (Redbooks) i serwisach WWW. Wszystkie pliki PDF można wyświetlić lub wydrukować.

Dokumentacja techniczna IBM (Redbooks)

- IBM System i Security Guide for IBM i5/OS Version 5 Release 4
- AS/400 Internet Security: Implementing AS/400 Virtual Private Networks
- AS/400 Internet Security Scenarios: A Practical Approach
- OS/400 V5R2 Virtual Private Networks: Remote Access to the IBM eServer iSeries Server with Windows 2000 VPN Clients

Serwisy WWW

- TCP/IP for i5/OS: Virtual Private Networking
- TCP/IP for i5/OS: RFC Documents

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 przesyłać na adres:

IBM Director of
Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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
Tokio 106-0032, Japonia

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 STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON 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 uwzględnione 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.

Licencjobiorcy 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 YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

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

Licencjonowany program opisany w niniejszym dokumencie 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, Umowie Licencyjnej IBM na Kod Maszynowy 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 możliwości 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.

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/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Informacje dotyczące interfejsu programistycznego

Niniejsza publikacja dotycząca sieci VPN stanowi dokumentację interfejsów programistycznych, które umożliwiają klientowi pisanie programów w celu uzyskania usług w systemie IBM i5/OS.

Znaki towarowe

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

Approach
AS/400
  Balance
eServer
  i5/OS
  IBM
  iSeries
  OS/400
  SAA
  System i

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

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

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

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

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 na ich podstawie 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 na podstawie tych publikacji ani ich fragmentów 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, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

Drukowane w USA