System i

Bezpečnosť
Virtuálne súkromné siete

Verzia 6 vydanie 1

System i

Bezpečnosť
Virtuálne súkromné siete

Verzia 6 vydanie 1

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si prečítajte informácie v časti “Poznámky”, na strane 77.

Toto vydanie sa vzťahuje na verziu 6, vydanie 1, modifikáciu 0 produktu IBM i5/OS (produktové číslo 5761-SS1) a na všetky jeho následné vydania a modifikácie, až kým to nebude v nových vydaniach uvedené inak. Táto verzie nebeží na všetkých modeloch počítačov typu RISC (Reduced Instruction Set Computer) a ani na modeloch CISC.

Obsah

Virtuálne súkromné siete

Virtuálna súkromná sieť (VPN) umožňuje vašej spoločnosti bezpečne rozširovať svoj súkromný intranet cez existujúci rámec verejnej siete, ako je internet. S VPN môže vaša spoločnosť riadiť prenos na sieti a súčasne zabezpečovať dôležité bezpečnostné funkcie, ako je autentifikácia a súkromie údajov.

VPN je voliteľne nainštalovateľný komponent System i Navigator, grafického užívateľského rozhrania (GUI) pre i5/OS. Tento umožňuje vytvárať bezpečnú cestu medzi dvomi koncami medzi akoukoľvek kombináciou hostiteľa a brány. VPN používa autentifikačné metódy, šifrovacie algoritmy a ďalšie bezpečnostné opatrenia, aby zaručilo, že údaje odosielané medzi dvoma koncovými bodmi ostanú zabezpečené.

VPN pracuje na sieťovej vrstve zásobníkového modelu vrstvenej komunikácie TCP/IP. VPN konkrétne používa otvorenú štruktúru Bezpečnostnej architektúry IP (IP Security Architecture, IPSec). IPSec zabezpečuje základné bezpečnostné funkcie pre internet, ako aj dodáva flexibilné stavebné bloky, z ktorých môžete vytvárať mohutné bezpečné virtuálne súkromné siete.

VPN podporuje aj riešenia VPN pre Tunelový protokol vrstvy 2 (L2TP). Pripojenia L2TP, nazývané tiež virtuálne linky, zabezpečujú cenovo efektívny prístup pre vzdialených užívateľov tak, že povoľujú podnikovému sieťovému serveru riadiť adresy IP priradené týmto vzdialeným užívateľom. Okrem toho pripojenia L2TP poskytujú bezpečný prístup do vášho systému alebo siete, keď ich chránite s IPSec.

Je dôležité, aby ste pochopili, že VPN bude mať vplyv na vašu celú sieť. Správne plánovanie a implementácia sú základom vášho úspechu. Prezrite si tieto témy, aby ste zistili ako VPN pracujú a ako ich môžete používať:

Čo je nové v V6R1

Prečítajte si, ktoré informácie súhrnu tém Virtuálne súkromné siete sú nové alebo významne zmenené.

Nová funkcia: IP verzia 6

Pri vytváraní VPN s nasledujúcimi typmi pripojení môžete teraz využívať protokol IP verzia 6: hostiteľ-hostiteľ, hostiteľ-brána a brána-brána. Pripojenia VPN podporujú využitie protokolu IP verzia 6 v adrese, rozsahu, podsieti a názve hostiteľa. Všetci sprievodcovia VPN boli aktualizovaní tak, aby akceptovali nové typy identifikátorov podľa protokolu IP verzia 6.

- Internetový protokol verzia 6

Ako zistiť, čo je nové alebo sa zmenilo

Na určenie miesta, na ktorom boli vykonané technické zmeny, sú v tomto dokumente použité:

- Značka  , ktorá označuje, kde začínajú nové alebo zmenené informácie.
- Značka  , ktorá označuje, kde nové alebo zmenené informácie končia.

Ak chcete nájsť ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené, pozrite si Poznámky pre užívateľov.

Súbor PDF k téme Virtuálna súkromná sieť

Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

Ak chcete tento dokument zobraziť alebo stiahnuť vo verzii PDF, vyberte tému Virtual private network (VPN)  (približne 1100 KB).

Uloženie súborov PDF

Ako uložiť PDF na vašu pracovnú stanicu na zobrazovanie alebo tlač:

1. Kliknite pravým tlačidlom myši na odkaz na PDF vo vašom prehliadači.
2. Ak používate program Internet Explorer, kliknite na **Uložiť cieľ ako** (Save Target As). Ak používate program Netscape Communicator, kliknite na **Uložiť odkaz ako** (Save Link As).
3. Prejdite do adresára, do ktorého chcete uložiť PDF.
4. Kliknite na **Uložiť**.

Stiahnutie programu Adobe Acrobat Reader

Aby ste mohli zobrazovať alebo tlačiť tieto dokumenty PDF, potrebujete program Adobe Acrobat Reader. Jeho kópiu si môžete stiahnuť na webových stránkach Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepty VPN

Je dôležité, aby ste pred implementáciou pripojenia VPN mali aspoň základnú znalosť štandardných technológií VPN.

Virtuálne súkromné siete (VPN) používajú na ochranu prenosu údajov niekoľko dôležitých protokolov TCP/IP. Ak chcete lepšie porozumieť fungovaniu pripojenia VPN, oboznámte sa s týmito protokolmi a konceptmi a s tým, ako ich používa VPN:

Bezpečnostné IP protokoly

IPSec (IP Security) poskytuje stabilný dlhodobý základ pre zabezpečenie bezpečnosti sieťových vrstiev.

IPSec podporuje všetky aktuálne používané kryptografické algoritmy a môže pojať aj novšie a výkonnejšie algoritmy, ak budú dostupné. Protokoly IPSec adresujú tieto hlavné bezpečnostné otázky:

Autentifikácia pôvodu údajov
Overuje, či každý datagram pochádza od vyhlasovaného odosielateľa.

Integrita údajov
Overuje, či sa obsah datagramu počas prenosu nezmenil, či už úmyselne alebo vplyvom náhodných chýb.

Utajenie údajov
Utajuje obsah správy, väčšinou pomocou šifrovania.

Ochrana opakovaného prehrávania
Zaisťuje, že útočník nemôže zachytiť datagram a prehrať ho niekedy neskôr.

Automatický manažment kryptografických kľúčov a bezpečnostných priradení
Uistite sa, že sa vaša politika VPN môže použiť v rozšírenej sieti s jednoduchou alebo nemanuálnou konfiguráciou.

VPN používa dva protokoly IPSec na ochranu údajov počas ich prenosu cez VPN: Authentication Header (AH) a Encapsulating Security Payload (ESP). Druhá časť povolenia IPSec je protokol Internet Key Exchange (IKE) alebo riadenie kľúčov. Zatiaľ čo IPSec šifruje vaše údaje, IKE podporuje automatizované vyjednávanie bezpečnostných asociácií (SA) a automatizované generovanie a obnovovanie šifrovacích kľúčov.

Poznámka: Bezpečnosť niektorých konfigurácií VPN môže byť zraniteľná v závislosti od konfigurácie IPSec. Táto zraniteľnosť postihuje konfigurácie, v ktorých je IPSec nakonfigurované na využitie protokolu ESP (Encapsulating Security Payload) v režime tunela s utajením (šifrovaním), ale bez ochrany integrity (autentifikácie) alebo protokolu AH (Authentication Header). Predvolená konfigurácia po vybratí ESP vždy zahrňuje autentifikačný algoritmus, ktorý poskytuje ochranu integrity. Preto pokiaľ nebude autentifikačný algoritmus v transformácii ESP odstránený, konfigurácie VPN budú chránené pred touto zraniteľnosťou. Konfigurácia univerzálneho pripojenia IBM VPN neovplyvní túto zraniteľnosť.

Ak chcete skontrolovať, či je váš systém postihnutý touto zraniteľnosťou, vykonajte tieto kroky:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → IP Security Policies → Data Policies** .
2. Pravým tlačidlom myši kliknite na politiku údajov, ktorú chcete skontrolovať a vyberte **Vlastnosti**.
3. Kliknite na záložku **Návrhy**.
4. Vyberte ktorýkoľvek z návrhov na ochranu údajov, ktorý používa protokol ESP a kliknite na **Upraviť**.
5. Kliknite na záložku **Transformácie**.
6. Zo zoznamu vyberte ľubovoľnú transformáciu, ktorá používa protokol ESP a kliknite na **Upraviť**.
7. Skontrolujte, že autentifikačný algoritmus má inú hodnotu než **Žiadny**.

Internet Engineering Task Force (IETF) formálne definuje IPSec v Požiadavke o komentár (Request for Comment, RFC) 2401, *Bezpečnostná architektúra pre Internetový protokol*. Toto RFC si môžete pozrieť na tejto webovej lokalite na Internete: http://www.rfc-editor.org.

Nasledujú základné protokoly IPSec:

Súvisiace koncepty

“Správa kľúčov” na strane 6
Dynamická VPN zabezpečuje dodatočnú bezpečnosť pre vašu komunikáciu pomocou protokolu Internet Key Exchange (IKE) pre správu kľúčov. IKE umožňuje VPN serverom na oboch koncoch pripojenia vyjednávať v určených intervaloch nové kľúče.

Súvisiace informácie

http://www.rfc-editor.org

Autentifikačná hlavička

Protokol Autentifikačná hlavička (AH) zabezpečuje autentifikáciu pôvodu údajov, integrity údajov a ochranu opakovaného prehrávania. AH však nezabezpečuje utajenie údajov, čo znamená, že všetky údaje sa posielajú bez úprav.

AH zaisťuje integritu údajov s kontrolným súčtom, ktorý generuje kód autentifikácie správy, ako je MD5. Ak chcete zaručiť autentifikáciu pôvodu údajov, AH zahrňuje tajný zdieľaný kľúč v algoritme, ktorý používa na autentifikáciu. Pre zaistenie ochrany opakovaného prehrávania, AH používa v hlavičke AH pole sekvenčného čísla. Stojí za zmienku, že tieto tri separátne funkcie sú zvyčajne zoradené za sebou a pri ich označení je využívané pomenovanie autentifikácia. Zjednodušene povedané, AH zaistí, aby cestou do cieľového bodu nedošlo k manipulácii s vašimi údajmi.

Hoci AH, pokiaľ ide o datagram IP, autentifikuje podľa možností maximum, hodnoty istých polí v hlavičke IP nemôže príjemca predvídať. Tieto polia, známe tiež ako premenlivé polia, protokol AH nechráni. AH však vždy ochraňuje užitočné zaťaženie paketu IP.

Internet Engineering Task Force (IETF) formálne definuje AH v Požiadavke o komentár (Request for Comment, RFC) 2402, *Autentifikačná hlavička IP*. Toto RFC si môžete pozrieť na tejto webovej lokalite na Internete: http://www.rfc-editor.org.

Spôsoby používania AH

AH môžete používať dvoma spôsobmi: v prenosovom režime alebo tunelovom režime. V prenosovom režime je hlavička IP datagramu najkrajnejšou hlavičkou IP, za ktorou nasleduje hlavička AH a potom užitočné zaťaženie datagramu. AH autentifikuje celý datagram okrem premenlivých polí. Informácie obsiahnuté v datagrame sa však prenášajú bez úprav, a preto sú náchylné na odpočúvanie. Prenosový režim vyžaduje menej dodatočného spracovania ako tunelový režim, ale neposkytuje takú vysokú bezpečnosť.

Tunelový režim vytvára hlavičky IP a používa ich ako najkrajnejšiu hlavičku IP datagramu. Hlavička AH nasleduje za hlavičkou IP. Pôvodný datagram (hlavička IP aj pôvodné užitočné zaťaženie) nasleduje ako posledný. AH autentifikuje celý datagram, čo znamená, že zodpovedajúci systém môže zistiť, či sa datagram po trase nezmenil.

Keď je jeden koniec bezpečnostnej autentifikácie bránou, použite tunelový režim. V tunelovom režime nemusia byť zdrojové a cieľové adresy v najkrajnejšej hlavičke IP zhodné s adresami v pôvodnej hlavičke IP. Tunel AH môžu napríklad obsluhovať dve bezpečnostné brány autentifikujúce všetky prenosy medzi sieťami, ktoré spájajú. V skutočnosti ide o dosť typickú konfiguráciu.

Hlavnou výhodou používania tunelového režimu je, že tunelový režim dokonale ochraňuje zapuzdrený datagram IP. Okrem toho tunelový režim umožňuje používanie súkromných adries.

Prečo AH?

V mnohých prípadoch vyžadujú vaše údaje len autentifikáciu. Protokol ESP (Encapsulating Security Payload) síce umožňuje vykonať autentifikáciu, ale AH na rozdiel od ESP neovplyvňuje až tak výkon systému. Ďalšou výhodou používania AH je, že AH autentifikuje celý datagram. ESP ale neautentifikuje počiatočnú hlavičku IP alebo žiadne ďalšie informácie, ktoré sa nachádzajú pred hlavičkou ESP.

ESP navyše vyžaduje na to, aby bol účinný, výkonné šifrovacie algoritmy. Výkonné šifrovanie je zakázané v niektorých regiónoch, zatiaľ čo AH nie je regulované a preto môže byť použité po celom svete.

Používanie ESN s AH

Ak používate protokol AH, môžete aktivovať ESN (Extended Sequence Number). ESN vám umožňuje prenášať veľký rozsah údajov vysokými rýchlosťami bez nutnosti prekľúčovania. Pripojenie VPN používa 64-bitové poradové čísla namiesto 32-bitových čísel cez protokol IPSec. Pri použití 64-bitových poradových čísel nie je potreba častého prekľúčovania, čím sa predchádza vyčerpaniu poradových čísel a minimalizuje sa používanie systémových prostriedkov.

Aký algoritmus používa AH na ochranu mojich informácií?

AH používa algoritmus známy ako **HMAC (Hashed Message Authentication Codes).** Konkrétne VPN používa buď HMAC-MD5 alebo HMAC-SHA. MD5 aj SHA zoberú vstupné údaje s premenlivou dĺžkou a tajný kľúč a vyprodukujú výstupné údaje s pevnou dĺžkou (nazývané transformačná hodnota). Ak sa transformácie dvoch správ zhodujú, je veľmi pravdepodobné, že správy sú rovnaké. MD5 aj SHA kódujú vo svojich výstupoch dĺžku správ, ale SHA sa považuje za bezpečnejšiu, lebo produkuje väčšie transformácie.

Internet Engineering Task Force (IETF) formálne definuje HMAC-MD5 v požiadavke o komentáre (Request for Comments, RFC) 2085, *Autentifikácia IP HMAC-MD5 s ochranou prehrávania*. Internet Engineering Task Force (IETF) formálne definuje HMAC-SHA v požiadavke o komentáre (Request for Comments, RFC) 2404, *Používanie HMAC-SHA-1-96 v ESP a AH*. Tieto dokumenty RFC si môžete pozrieť na tejto webovej lokalite na Internete: http://www.rfc-editor.org.

Súvisiace koncepty

"Zapuzdrovanie bezpečnostného užitočného zaťaženia"
Protokol Zapuzdrovanie bezpečnostného užitočného zaťaženia (Encapsulating Security Payload, ESP) zabezpečuje dôvernosť údajov a voliteľne zabezpečuje aj autentifikáciu pôvodu údajov, kontrolu integrity údajov a ochranu opakovaného prehrávania.

Súvisiace informácie

http://www.rfc-editor.org

Zapuzdrovanie bezpečnostného užitočného zaťaženia

Protokol Zapuzdrovanie bezpečnostného užitočného zaťaženia (Encapsulating Security Payload, ESP) zabezpečuje dôvernosť údajov a voliteľne zabezpečuje aj autentifikáciu pôvodu údajov, kontrolu integrity údajov a ochranu opakovaného prehrávania.

Rozdiel medzi protokolmi ESP a AH (Authentication Header) je ten, že ESP poskytuje šifrovanie, pričom oba protokoly poskytujú autentifikáciu, kontrolu integrity a ochranu opakovaného prehrávania. S ESP oba komunikujúce systémy používajú na šifrovanie a dešifrovanie vymieňaných údajov zdieľaný kľúč.

AK sa rozhodnete použiť šifrovanie a autentifikáciu, odpovedajúci systém najskôr autentifikuje paket a potom, ak je prvý krok úspešný, systém pristúpi k šifrovaniu. Tento typ konfigurácie redukuje prídavne spracovanie, ako aj redukuje vašu zraniteľnosť pred útokmi typu odmietnutie služby.

Dva spôsoby používania ESP

ESP môžete používať dvomi spôsobmi: v prenosovom režime alebo tunelovom režime. V prenosovom režime hlavička ESP nasleduje za hlavičkou IP pôvodného datagramu IP. Ak datagram už má hlavičku IPSec, hlavička ESP bude pred ňou. Príves ESP a voliteľná autentifikácia údajov nasledujú za užitočným zaťažením.

Prenosový režim neautentifikuje ani nešifruje hlavičku IP, ktorá môže pri prenose datagramu odhaľovať vaše adresovacie informácie potencionánym narušiteľom. Prenosový režim vyžaduje menej dodatočného spracovania ako tunelový režim, ale neposkytuje takú vysokú bezpečnosť. Vo väčšine prípadov hostitelia používajú ESP v prenosovom režime.

Tunelový režim vytvára hlavičky IP a používa ich ako najkrajnejšiu hlavičku IP datagramu, za ktorou nasleduje hlavička ESP a potom pôvodný datagram (hlavička IP aj pôvodné užitočné zaťaženie). Príves ESP a voliteľná autentifikácia údajov sa pripoja k užitočnému zaťaženiu. Keď používate autentifikáciu aj šifrovanie, ESP úplne ochraňuje pôvodný datagram, lebo teraz sú to údaje užitočného zaťaženia pre nový paket ESP. ESP ale nechráni novú hlavičku IP. Brány musia používať ESP v tunelovom režime.

Aký algoritmus používa ESP na ochranu mojich informácií?

ESP používa symetrický kľúč, ktorý obe komunikujúce strany používajú na šifrovanie a dešifrovanie vymieňaných údajov. Odosielateľ a príjemca sa musia predtým, ako sa medzi nimi uskutoční bezpečná komunikácia, dohodnúť na kľúči. VPN používa na šifrovanie štandardy DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 alebo AES (Advanced Encryption Standard).

Ak ako šifrovací algoritmus vyberiete algoritmus AES, môžete aktivovať ESN (Extended Sequence Number). ESN vám umožňuje prenášať veľký rozsah údajov vysokými rýchlosťami. Pripojenie VPN používa 64-bitové poradové čísla namiesto 32-bitových čísel cez protokol IPSec. Pri použití 64-bitových poradových čísel nie je potreba častého prekľúčovania, čím sa predchádza vyčerpaniu poradových čísel a minimalizuje sa používanie systémových prostriedkov.

Internet Engineering Task Force (IETF) formálne definuje DES v Požiadavke o komentár (Request for Comment, RFC) 1829, *Transformácia ESP DES-CBC*. IETF formálne definuje 3DES v RFC 1851, *The ESP Triple DES Transform*. Tieto a iné dokumenty RFC si môžete pozrieť na tejto webovej adrese na Internete: http://www.rfc-editor.org.

ESP používa na zabezpečenie autentifikačných funkcií algoritmy HMAC-MD5 a HMAC-SHA. MD5 aj SHA zoberú vstupné údaje s premenlivou dĺžkou a tajný kľúč a vyprodukujú výstupné údaje s pevnou dĺžkou (nazývané transformačná hodnota). Ak sa transformácie dvoch správ zhodujú, je veľmi pravdepodobné, že správy sú rovnaké. MD5 aj SHA kódujú vo svojich výstupoch dĺžku správ, ale SHA sa považuje za bezpečnejšiu, lebo produkuje väčšie transformácie.

IETF formálne definuje HMAC-MD5 v RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. IETF formálne definuje HMAC-SHA v RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Tieto a iné dokumenty RFC si môžete pozrieť na tejto webovej adrese na Internete: http://www.rfc-editor.org.

Súvisiace koncepty

“Autentifikačná hlavička” na strane 3
Protokol Autentifikačná hlavička (AH) zabezpečuje autentifikáciu pôvodu údajov, integrity údajov a ochranu opakovaného prehrávania. AH však nezabezpečuje utajenie údajov, čo znamená, že všetky údaje sa posielajú bez úprav.

Súvisiace informácie

http://www.rfc-editor.org

Skombinované AH a ESP

VPN umožňuje kombinovať AH a ESP pre pripojenia typu hostiteľ-hostiteľ v prenosovom režime.

Kombinácia týchto protokolov ochraňuje celý datagram IP. Aj napriek tomu, že kombinácia dvoch protokolov ponúka vyššiu bezpečnosť, prináša so sebou aj zvýšené nároky na spracovanie, ktoré môžu prevážiť jej výhody.

Správa kľúčov

Dynamická VPN zabezpečuje dodatočnú bezpečnosť pre vašu komunikáciu pomocou protokolu Internet Key Exchange (IKE) pre správu kľúčov. IKE umožňuje VPN serverom na oboch koncoch pripojenia vyjednávať v určených intervaloch nové kľúče.

Pri každom úspešnom vyjednávaní vygenerujú servery VPN kľúče, ktoré ochraňujú pripojenie, a takto sťažujú útočníkovi zachytiť informácie z pripojenia. Navyše, ak používate dokonalé utajenie postupovania, útočníci nemôžu odvodiť budúce kľúče na základe informácií z predchádzajúcich kľúčov.

Správca kľúčov VPN je implementáciou protokolu IKE (Internet Key Exchange) spoločnosťou IBM. Správca kľúčov podporuje automatické vyjednávanie bezpečnostných asociácií (SA), ako aj automatické generovanie a obnovu šifrovacích kľúčov.

Bezpečnostná asociácia (SA) obsahuje informácie o tom, čo je nevyhnutné na používanie protokolov IPSec. SA napríklad identifikuje typy algoritmov, dĺžky kľúčov a doby ich existencie, zúčastnené strany a režimy zapuzdrovania.

Šifrovacie kľúče, ako už naznačuje názov, zamykajú či ochraňujú vaše informácie, kým bezpečne nedosiahnu svoj konečný cieľ.

Poznámka: Bezpečné generovanie vašich kľúčov je najdôležitejším faktorom pri vytváraní bezpečného a súkromného pripojenia. Ak sú vaše kľúče skompromitované, vaše úsilie o autentifikáciu a šifrovanie, bez ohľadu na ich odolnosť, bude zbytočné.

Fázy manažmentu kľúčov

Správca kľúčov VPN používa vo svojej implementácii dve rôzne fázy.

Fáza 1 Fáza 1 vytvorí hlavný tajný kľúč, z ktorého sa odvodzujú ďalšie šifrovacie kľúče na ochranu prenosu užívateľských údajov. Takto to prebieha, aj keď medzi dvomi koncovými bodmi ešte neexistuje žiadna bezpečnostná ochrana. VPN používa na autentifikáciu vyjednávaní fázy 1, ako aj na vytváranie kľúčov na ochranu správ IKE, ktoré sa prenášajú počas nasledujúcich vyjednávaní fázy 2, buď podpisový režim RSA alebo dopredu zdieľané kľúče.

Dopredu zdieľaný kľúč je netriviálny reťazec s dĺžkou až 128 znakov. Obidva koncové body pripojenia sa musia zhodovať na dopredu zdieľanom kľúči. Výhoda používania dopredu zdieľaných kľúčov je v ich jednoduchosti, nevýhodou je to, že zdieľané tajnosti musia byť pred dohodovaniami IKE distribuované von-z-pásma, napríklad cez telefón alebo zaregistrovaný e-mail. Ako heslo použite váš dopredu zdieľaný kľúč.

Autentifikácia *Podpisu RSA* zabezpečuje vyššiu bezpečnosť ako dopredu zdieľaný kľúč, lebo tento režim na zabezpečovanie autentifikácie používa digitálne certifikáty. Vaše digitálne certifikáty musíte nakonfigurovať pomocou správcu digitálnych certifikátov. Okrem toho niektoré riešenia VPN vyžadujú pre prevádzkyschopnosť Podpis RSA. Napríklad Windows 2000 VPN používa podpis RSA

ako svoju predvolenú metódu autentifikácie. Nakoniec, podpis RSA poskytuje väčšiu škálovateľnosť ako dopredu zdieľané kľúče. Certifikáty, ktoré používate, musia pochádzať od certifikačných autorít, ktorým dôverujú oba servery.

Fáza 2 Fáza 2 dohoduje bezpečnostné asociácie a kľúče, ktoré ochraňujú aktuálne výmeny údajov aplikácie. Nezabudnite, že až do tohto momentu sa žiadne aplikačné údaje vlastne neodoslali. Fáza 1 ochraňuje správy IKE fázy 2.

Keď sú vyjednávania fázy 2 dokončené, vaša VPN vytvorí bezpečné dynamické pripojenie cez sieť a medzi koncovými bodmi, ktoré ste definovali pre vaše pripojenie. Všetky údaje, ktoré sa presúvajú cez VPN sú doručené so stupňom zabezpečenia a efektivity odsúhlaseným kľúčovými servermi počas fázy 1 a fázy 2 vyjednávacieho procesu.

Vo všeobecnosti prebiehajú vyjednávania fázy 1 raz denne, zatiaľ čo vyjednávania fázy 2 sa obnovujú každých 60 minút alebo aj každých 5 minút. Vyššia frekvencia obnovovania zvyšuje bezpečnosť vašich údajov, ale znižuje výkon systému. Na ochranu vašich najcitlivejších údajov použite krátke doby existencie kľúčov.

Ak vytvoríte dynamické VPN pomocou System i Navigator, musíte definovať politiku IKE, aby ste povolili dohodovanie fázy 1 a politiku údajov, čo umožňuje prejsť k dohodovaniu fázy 2. Voliteľne môžete použiť sprievodcu Nové pripojenie. Sprievodca automaticky vytvorí každý z objektov konfigurácie, ktoré VPN vyžaduje pre svoju správnu činnosť, vrátane politiky IKE a údajovej politiky.

Odporúčané čítanie

Ak máte záujem o viac informácií o protokole Internet Key Exchange (IKE) a správe kľúčov, pozrite si tieto požiadavky na komentáre (RFC) pre Internet Engineering Task Force (IETF):

- 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)*

Tieto dokumenty RFC si môžete pozrieť na tejto webovej lokalite na Internete: http://www.rfc-editor.org.

Súvisiace koncepty

“Scenár: VPN využívajúca firewally” na strane 28
V tomto scenári chce veľká poisťovacia spoločnosť vytvoriť VPN medzi bránou v Chicagu a hostiteľom v Minneaplise, pričom obe siete sa nachádzajú za firewallom.

“Bezpečnostné IP protokoly” na strane 2
IPSec (IP Security) poskytuje stabilný dlhodobý základ pre zabezpečenie bezpečnosti sieťových vrstiev.

Súvisiace úlohy

“Konfigurácia politiky IKE (Internet Key Exchange)” na strane 46
Politika IKE (Internet Key Exchange) definuje, akú úroveň ochrany autentifikáciou a šifrovaním využíva IKE počas 1 fázy vyjednávania.

“Konfigurácia údajovej politiky” na strane 47
Údajová politika definuje, aká úroveň autentifikácie alebo šifrovania ochraňuje údaje počas ich prenosu cez VPN.

Súvisiace informácie

http://www.rfc-editor.org

Protokol L2TP (Layer 2 Tunnel Protocol)

Pripojenia L2TP (Layer 2 Tunneling Protocol), nazývané aj virtuálne linky, umožňujú, aby podnikové sieťové systémy riadili IP adresy priradené vzdialeným užívateľom, vďaka čomu týmto vzdialeným užívateľom poskytujú cenovo výhodný prístup. Okrem toho pripojenia L2TP poskytujú bezpečný prístup do vášho systému alebo siete, keď ich používate v spojení s Bezpečnosťou IP (IPSec)

L2TP podporuje dva tunelové režimy: dobrovoľný tunel a povinný tunel. Hlavným rozdielom medzi týmito dvoma tunelovými režimami je koncový bod. V prípade dobrovoľného tunela ide o zakončenie na vzdialenom klientovi, zatiaľ čo povinný tunel je zakončený u poskytovateľa internetových služieb (ISP).

Pri **povinnom tuneli** L2TP iniciuje vzdialený hostiteľ pripojenie ku svojmu ISP. ISP potom vytvorí pripojenie L2TP medzi vzdialeným užívateľom a podnikovou sieťou. Hoci ISP vytvorí pripojenie, vy rozhodujete o tom, ako ochrániť prenos pomocou VPN. S povinným tunelom musí ISP podporovať LT2P.

S **dobrovoľným tunelom** L2TP, pripojenie vytvorí vzdialený užívateľ, väčšinou pomocou tunelovacieho klienta L2TP. Následkom toho vzdialený užívateľ odošle pakety L2TP svojmu ISP, ktorý ich postúpi ďalej do podnikovej siete. S dobrovoľným tunelom nemusí ISP podporovať L2TP. V scenári Ochrana nevynúteného tunela L2TP pomocou IPSec nájdete príklad na konfiguráciu kancelárskeho systému pobočky na pripojenie k svojej firemnej sieti cez systém brány pomocou tunela L2TP, ktorý zabezpečuje VPN.

Môžete zobraziť vizuálnu prezentáciu o koncepte nevynútených tunelov L2TP chránených protokolom IPSec. Toto vyžaduje doplnkový komponent Flash. Prípadne môžete použiť HTML verziu tejto prezentácie.

L2TP je v skutočnosti obmena protokolu zapuzdrovania IP. Tunel L2TP sa vytvára zapuzdrovaním rámika L2TP do paketu protokolu User Datagram Protocol (UDP), ktorý sa zase zapuzdruje do paketu IP. Zdrojové a cieľové adresy tohto paketu IP definujú koncové body pripojenia. Keďže vonkajší zapuzdrovací protokol je IP, môžete protokoly IPSec použiť na zložený paket IP. Takto sa ochránia údaje, ktoré sa prenášajú tunelom L2TP. Potom môžete priamym spôsobom použiť protokol Authentication Header (AH), Encapsulated Security Payload (ESP) a Internet Key Exchange (IKE).

Súvisiace koncepty

"Scenár: Ochrana dobrovoľného tunela L2TP protokolom IPSec" na strane 21
V tomto scenári sa oboznámite so spôsobom nastavenia pripojenia medzi kancelárskym hostiteľom pobočky a centrály, ktoré používa L2TP chránené pomocou IPSec. Pobočka má dynamicky priradenú adresu IP, zatiaľ čo centrála spoločnosti má statickú, globálne smerovateľnú adresu IP.

Preklad sieťových adries pre VPN

VPN poskytuje prostriedky na preklad sieťových adries nazývaný VPN NAT. VPN NAT sa líši od zvyčajného NAT v tom, že prekladá adresy pred použitím protokolov IKE a IPSec. Obráťte sa na túto tému, v ktorej sa dozviete viac.

Preklad sieťových adries (NAT) vezme vaše súkromné adresy IP a preloží ich do verejných adries IP. To pomáha zachovávať hodnotné verejné adresy a súčasne umožňuje hostiteľom vo vašej sieti pristupovať k službám a vzdialeným hostiteľom cez Internet (alebo inú verejnú sieť).

Okrem toho, ak používate súkromné adresy IP, tieto môžu byť v konflikte s podobnými prichádzajúcimi adresami IP. Môžete napríklad chcieť komunikovať s inou sieťou, ktorá ale používa adresy 10.*.*.*, čo spôsobí kolízie adries a ukončenie všetkých paketov. Tento problém môžte vyriešiť použitím NAT na odchádzajúce adresy. Ak je ale prenos údajov chránený pomocou VPN, obvyklý NAT nebude fungovať, lebo mení adresy IP v bezpečnostných asociáciách (SA), ktoré VPN vyžaduje pre svoju činnosť. Aby ste sa tomuto problému vyhli, VPN zabezpečuje svoju vlastnú verziu prekladu sieťových adries nazývanú VPN NAT. VPN NAT vykonáva preklad adries pred kontrolou platnosti SA pomocou priraďovania adresy k pripojeniu, keď sa pripojenie spustí. Adresa zostáva priradená k pripojeniu, kým toto pripojenie nevymažete.

Poznámka: FTP v tomto čase ešte nepodporuje VPN NAT.

Ako mám použiť VPN NAT?

Sú dva rozličné typy VPN NAT, ktoré musíte vziať do úvahy, kým začnete. Sú to:

VPN NAT na predchádzanie konfliktom adries IP

Tento typ VPN NAT umožňuje vyhnúť sa možným konfliktom adries IP, keď konfigurujete pripojenie VPN medzi sieťami alebo systémami s podobnými schémami adresovania. Typický návrh je, keď obe spoločnosti chcú vytvoriť pripojenia VPN pomocou jedného zo stanovených rozsahov súkromných adries IP. Napríklad 10.*.*.*. Spôsob konfigurácie tohto typu VPN NAT je závislý na tom, či v

prípade tohto pripojenia VPN je váš systém iniciátorom alebo odpovedačom. Ak je váš systém iniciátorom pripojenia, môžete vaše lokálne adresy prekladať do adries, ktoré sú kompatibilné s adresami vášho partnera v pripojení VPN. Ak je váš systém odpovedačom pripojenia, môžete vzdialené adresy partnera VPN prekladať do adries, ktoré sú kompatibilné s vašou lokálnou schémou adresovania. Tento typ prekladu adries nakonfigurujte len pre svoje dynamické pripojenia.

VPN NAT na skrytie lokálnych adries

Tento typ VPN NAT sa používa predovšetkým na skrytie skutočnej adresy IP vášho lokálneho systému pomocou prekladu jeho adresy na inú adresu, ktorú verejne sprístupníte. Keď konfigurujete VPN NAT, môžete určiť, aby sa každá verejne známa adresa IP prekladala na jednu z množstva skrytých adries. Toto tiež umožňuje vyrovnávať prenosové zaťaženie pre jednotlivú adresu v rámci viacerých adries. VPN NAT pre lokálne adresy vyžaduje, aby váš systém v tomto pripojení vystupoval ako odpovedač.

VPN NAT môžete používať na skrývanie lokálnych adries, ak odpoviete áno na tieto otázky:

1. Máte jeden alebo viac systémov, ku ktorým chcete ľuďom umožniť prístup prostredníctvom VPN?
2. Potrebujete byť flexibilní čo sa týka aktuálnych adries IP vášho systému?
3. Máte jednu alebo viac globálne smerovateľných adries IP?

Scenár Použitie prekladov sieťových adries v pripojení VPN vám poskytuje príklad, ako nakonfigurovať VPN NAT tak, aby ukryl lokálne adresy vo vašom modeli System i.

Podrobné pokyny ku konfigurácii VPN NAT vo vašom systéme nájdete v online pomoci dostupnej pre rozhranie VPN v System i Navigator.

Súvisiace koncepty

“Scenár: Použitie prekladania sieťových adries v pripojení VPN” na strane 38
V tomto scenári chce vaša spoločnosť vymeniť citlivé údaje s jedným zo svojich obchodných partnerov pomocou VPN. Aby spoločnosť ešte lepšie ochránila súkromie vlastnej štruktúry siete, použije VPN NAT na ukrytie súkromnej adresy IP systému, ktorý sa používa na hosťovanie aplikácií, ku ktorým má váš obchodný partner prístup.

“Plánovací pracovný list manuálneho pripojenia” na strane 43
Pred konfiguráciou manuálneho pripojenia vyplňte tento pracovný list.

IPSec s UDP kompatibilné s NAT

Zapuzdrenie UDP umožňuje prenosu IPSec prechádzať konvenčným zariadením NAT. Prezrite si túto tému, v ktorej nájdete viac informácií o tom, čo to je a prečo by ste to mali používať pre vaše pripojenia VPN.

Problém: Konvenčné NAT zabraňuje VPN

Preklad sieťových adries (NAT) umožňuje skryť vaše neregistrované súkromné adresy IP za množinu registrovaných adries IP. Toto pomáha ochraňovať vašu internú sieť pred vonkajšími sieťami. NAT tiež pomáha zmierňovať problém spotrebovania adries IP, keďže množstvo súkromných adries možno reprezentovať malou množinou registrovaných adries.

Nanešťastie obvyklý NAT nefunguje na paketoch IPSec, lebo keď paket prechádza zariadením NAT, zdrojová adresa sa v pakete zmení, a tým urobí paket neplatným. V takomto prípade prijímajúci koniec pripojenia VPN zruší paket a vyjednávania pripojenia VPN zlyhajú.

Riešenie: Zapuzdrenie UDP

Jedným slovom, zapuzdrenie UDP zabalí paket IPSec do novej, ale duplicitnej hlavičky IP/UDP. Adresa v novej hlavičke IP sa preloží, keď prechádza zariadením NAT. Potom ako paket dorazí na miesto určenia, prijímajúca strana zruší dodatočnú hlavičku a ponechá originálny paket IPSec, ktorý teraz prejde všetkými ostatnými validáciami.

UDP môžete použiť len na tie VPN, ktoré budú používať IPSec ESP v tunelovom alebo prenosovom režime. Navyše systém môže pri zapuzdrení UDP vystupovať len ako klient. Teda môže len *zahajovať* zapuzdrený prenos UDP.

Nasledujúci obrázok ilustruje formát paketu ESP zapuzdreného UDP v tunelovom režime:

Originálny datagram IPv4:

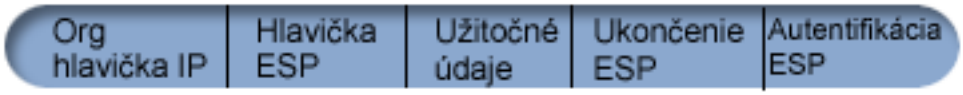
Po použití IPSec ESP v režime tunela:

Po použití zapuzdrenia UDP:

Nasledujúci obrázok ilustruje formát paketu ESP zapuzdreného UDP v prenosovom režime:

Originálny datagram IPv4:

Po použití IPSec ESP v prenosovom režime:



Po použití zapuzdrenia UDP:

Po zapuzdrení paketu systém odošle tento paket svojmu partnerovi VPN prostredníctvom portu UDP číslo 4500. Zvyčajne VPN partneri vykonávajú vyjednávania IKE cez UDP, port 500. Keď ale IKE zistí počas vyjednávania kľúčov NAT, odošlú sa ďalšie pakety IKE cez zdrojový port 4500, cieľový port 4500. Toto tiež znamená, že port 4500 nesmie byť obmedzený v žiadnych použiteľných filtrovacích pravidlách. Prijímajúci koniec pripojenia môže určiť, či je paket paketom IKE alebo zapuzdrený paket UDP, pretože prvé 4 bajty nákladov UDP sú nastavené na nulu na pakete IKE. Aby mohlo toto fungovať, oba konce pripojenia musia podporovať zapuzdrenie UDP.

Súvisiace koncepty

"Scenár: VPN využívajúca firewally" na strane 28
V tomto scenári chce veľká poisťovacia spoločnosť vytvoriť VPN medzi bránou v Chicagu a hostiteľom v Minneaplise, pričom obe siete sa nachádzajú za firewallom.

Komprimácia IP

Protokol IP Payload Compression (IPComp) zmenšuje veľkosť datagramov IP pomocou komprimácie datagramov za účelom zväčšenia komunikačného výkonu medzi dvoma partnermi.

Zámerom je zväčšiť celkový komunikačný výkon, keď komunikácia prebieha cez pomalé alebo preplnené linky. IPComp nezaručuje žiadnu bezpečnosť a musí sa používať spolu s transformáciou AH alebo ESP, keď sa na pripojení VPN vyskytne komunikácia.

Internet Engineering Task Force (IETF) formálne definuje IPComp v požiadavke o komentáre (RFC) 2393, *Protokol komprimácie užitočného zaťaženia IP (IPComp)*. Toto RFC si môžete pozrieť na tejto webovej lokalite na Internete: http://www.rfc-editor.org.

Súvisiace informácie

http://www.rfc-editor.org

Filtrovanie VPN a IP

Filtrovanie IP a VPN spolu tesne súvisia. V skutočnosti väčšina pripojení VPN vyžaduje, aby pravidlá pre filtre pracovali správne. Táto téma poskytuje informácie o tom, čo vyžadujú filtre VPN, ako aj ostatné koncepty filtrovania súvisiace s VPN.

Väčšina VPN spojení vyžaduje správne fungovanie filtrovacích pravidiel. Vyžadované pravidlá pre filtre závisia od typu pripojenia VPN, ktoré práve konfigurujete, ako aj od typu prenosu, ktorý chcete riadiť. Vo všeobecnosti každé pripojenie bude mať filter politiky. Filter politiky definuje, ktoré adresy, protokoly a porty môžu používať VPN. Navyše spojenia podporujúce protokol Internet Key Exchange (IKE) majú zvyčajne pravidlá, ktoré sú explicitne napísané tak, aby povoľovali spracovanie IKE cez spojenie. VPN môže tieto pravidlá generovať automaticky. Kedykoľvek je to možné, povoľte VPN, aby vám generovala filtre politík. Pomôže to nielen pri odstránení chýb, ale odstráni to aj potrebu nakonfigurovania pravidiel v samostatnom kroku pomocou editora Pravidiel pre pakety v System i Navigator.

Existujú samozrejme výnimky. V týchto témach nájdete bližšie informácie o ďalších, menej známych základných pojmoch VPN a filtrovania a o technikách, ktoré môžete využiť konkrétne vo vašej situácii:

Súvisiace koncepty

“Konfigurácia pravidiel pre pakety VPN” na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Pripojenia VPN bez filtrov politiky

Ak koncové body pripojenia vašej VPN sú jednoduché, presné adresy IP a chcete spustiť VPN bez toho, aby ste museli na systéme zapisovať alebo aktivovať pravidlá pre filtre, môžete nakonfigurovať dynamické filtre politiky.

Pravidlo filtra politiky definuje, ktoré adresy, protokoly a porty, môžu používať VPN a nasmeruje príslušný prenos cez toto pripojenie. V niektorých prípadoch budete možno chcieť nakonfigurovať pripojenie, ktoré nevyžaduje politiku pravidiel filtrovania. Môžete mať napríklad v rozhraní zavedené pravidlá pre pakety iných pripojení, ktoré použije aj vaše pripojenie VPN, a tak namiesto toho, aby ste deaktivovali aktívne pravidlá v tomto rozhraní, rozhodnete sa nakonfigurovať VPN tak, aby všetky filtre pripojenia dynamicky riadil váš systém. Na filter politiky pre tento typ pripojenia sa odkazuje ako na **dynamický filter politiky**. Kým budete môcť začať používať dynamický filter politiky pre vaše pripojenie VPN, všetky nasledujúce tvrdenia musia byť pravdivé:

- Toto pripojenie môže iniciovať len lokálny systém.
- Údajové koncové body pripojenia musia byť jednoduché systémy. Teda nemôžu to byť podsiete alebo rozsah adries.
- Pre pripojenie nemožno zaviesť žiadne pravidlo pre filtre politiky.

Ak vaše pripojenie vyhovuje týmto kritériám, môžete nakonfigurovať pripojenie tak, aby nevyžadovalo filter politiky. Keď sa pripojenie spustí, prenos medzi koncovými bodmi bude existovať bez ohľadu na to, aké iné pravidlá pre pakety sú na vašom systéme zavedené.

Podrobný návod na konfiguráciu pripojenia nevyžadujúce filter politiky nájdete v online pomoci pre VPN.

Implicitná IKE

Aby vo vašej VPN mohlo fungovať vyjednávanie IKE (Internet Key Exchange), musíte pre tento typ IP prenosov umožniť prenos datagramov UDP cez port 500. Ale ak nie sú na systéme žiadne pravidlá pre filtre konkrétne napísané na povolenie prenosu IKE, systém implicitne povolí tok prenosu IKE.

Aby bolo možné vytvoriť pripojenie, vyžaduje väčšina VPN, aby predtým, než bude môcť prebehnúť spracovanie IPSec, došlo najprv k vyjednávaniam IKE. IKE používa známy port 500, takže aby IKE pracovala správne, musíte povoliť datagramy UDP cez port 500 pre tento typ prenosu IP. Ak nie sú na systéme napísané žiadne filtrovacie pravidlá na povolenie prenosu IKE, potom je prenos IKE implicitne povolený. Pravidlá napísané špeciálne pre prenos UDP cez port 500 sú obsluhované podľa toho, čo je zadefinované v aktívnych filtrovacích pravidlách.

Scenáre: VPN

Pozrite si scenáre, aby ste sa oboznámili s technickými a konfiguračnými detailmi každého z týchto základných typov pripojení.

Súvisiace koncepty

Scenár QoS: bezpečné a očakávané výsledky (VPN a QoS)

Súvisiace informácie

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

Návrh: Základné pripojenie pobočky

V tomto návrhu chce vaša spoločnosť prostredníctvom páru modelov System i vystupujúcich ako brány VPN vytvoriť VPN medzi podsieťami dvoch vzdialených oddelení.

Situácia

Predpokladajme, že vaša spoločnosť chce minimalizovať výdaje vynakladané na komunikáciu s vlastnými pobočkami i medzi nimi. V súčasnosti vaša spoločnosť používa linky so snímkovým relé alebo prenajaté linky, ale chcete vyskúšať aj iné možnosti na prenos interných dôverných údajov, ktoré sú lacnejšie, bezpečnejšie a globálne prístupné. Pomocou internetu môžete jednoducho vytvoriť virtuálnu súkromnú sieť (Virtual private network, VPN), ktorá bude vyhovovať potrebám vašej spoločnosti.

Vaša spoločnosť i jej pobočka budú vyžadovať ochranu VPN cez internet, no nie medzi jednotlivými intranetmi. Keďže svoje intranety považujete za dôveryhodné, najlepším riešením je vytvoriť VPN typu brána-brána. V tomto prípade sú obe brány pripojené priamo na sprostredkovateľskú sieť. Inými slovami, sú *hraničnými* alebo *okrajovými* systémami, ktoré nie sú chránené firewallom. Tento príklad slúži ako vhodný úvod ku krokom potrebným na nastavenie základnej konfigurácie VPN. Ak sa tento scenár odvoláva na pojem *Internet*, znamená to sprostredkovateľskú sieť medzi dvoma VPN bránami, ktoré môžu byť podnikovou súkromnou sieťou alebo verejným internetom.

Dôležité: V tomto návrhu sú bezpečnostné brány modelu System i pripojené priamo k internetu. Nie je tu firewall kvôli zjednodušeniu návrhu. Neznamená to, že použitie firewallu nie je nevyhnutné. Zvážte si bezpečnostné riziká pripojenia k internetu.

Výhody

Tento návrh má nasledujúce výhody:

- Používanie internetu alebo existujúceho intranetu znižuje výdaje na súkromné linky medzi vzdialenými podsieťami.

- Používanie internetu alebo existujúceho intranetu znižuje zložitosť inštalácie a údržby súkromných liniek a pridruženého príslušenstva.
- Používanie internetu umožňuje pripojenie vzdialených sídiel takmer kdekoľvek vo svete.
- Použitie VPN poskytuje užívateľom prístup ku všetkým systémom a prostriedkom na oboch stranách pripojenia, akoby boli pripojení prostredníctvom prenajatej linky alebo siete WAN (wide area network).
- Používanie metód šifrovania a autentifikácie podľa priemyselných štandardov zaisťuje bezpečnosť citlivých informácií, ktoré sa odovzdávajú z jedného miesta na druhé.
- Dynamická a pravidelná výmena šifrovacích kľúčov zjednodušuje a minimalizuje riziko ich dekódovania, a tým porušenia vašej bezpečnosti.
- Používanie privátnych IP adries v každej vzdialenej podsieti prináša potrebu alokovania verejných IP adries pre každého klienta.

Ciele

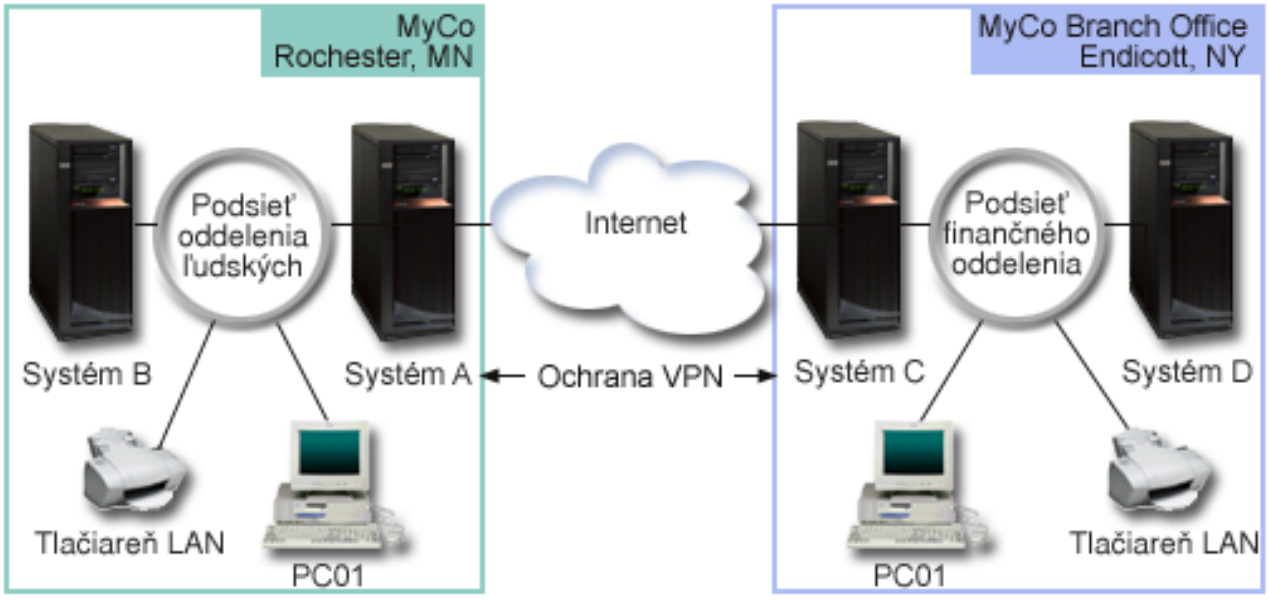
V tomto návrhu chce spoločnosť MyCo, Inc. vytvoriť VPN medzi podsieťou Oddelenia ľudských zdrojov a podsieťou Finančného oddelenia, a to prostredníctvom páru modelov System i. Oba systémy budú vystupovať ako brány VPN. V termínoch konfigurácií VPN brána vykoná správu kľúčov a aplikuje IPSec na údaje, ktoré sa prenášajú tunelom. Brány nie sú koncovými bodmi pripojenia.

Ciele tohto návrhu sú nasledujúce:

- VPN musí ochraňovať všetok prenos údajov medzi podsieťou personálneho oddelenia a podsieťou finančného oddelenia.
- Prenos údajov nevyžaduje ochranu VPN, keď dosiahne jednu z podsietí oddelenia.
- Všetci klienti a hostitelia na každej sieti majú úplný prístup k sieťam ostatných, vrátane všetkých aplikácií.
- Systémy brán môžu vzájomne komunikovať a navzájom pristupovať k aplikáciám druhej strany.

Detaily

Nasledujúci obrázok ilustruje charakteristiky siete spoločnosti MyCo.



Oddelenie ľudských zdrojov

- Systém A je spustený na i5/OS verzia 5 vydanie 3 (V5R3) alebo novšia a vystupuje ako brána VPN Oddelenia ľudských zdrojov.
- Podsieť je 10.6.0.0 s maskou 255.255.0.0. Táto podsieť reprezentuje koncový bod údajov tunela VPN v lokalite MyCo Rochester.
- Systém A je k internetu pripojený s IP adresou 204.146.18.227. Toto je koncový bod pripojenia. To znamená, že Systém A vykonáva riadenie kľúčov a na prichádzajúce a odchádzajúce datagramy využíva protokol IPSec.
- Systém A je k svojej podsieti pripojený s IP adresou 10.6.11.1.
- Systém B je produkčný systém v podsieti Ľudských zdrojov, v ktorej sú spustené štandardné aplikácie TCP/IP.

Finančné oddelenie

- Systém C je spustený na i5/OS verzia 5 vydanie 3 (V5R3) alebo novšia a vystupuje ako brána VPN Finančného oddelenia.
- Podsieť je 10.196.8.0 s maskou 255.255.255.0. Táto podsieť reprezentuje koncový bod údajov tunela VPN na lokalite MyCo Endicott.
- Systém C je k internetu pripojený s IP adresou 208.222.150.250. Toto je koncový bod pripojenia. To znamená, že Systém C vykonáva riadenie kľúčov a na prichádzajúce a odchádzajúce datagramy využíva protokol IPSec.
- Systém C je k svojej podsieti pripojený s IP adresou 10.196.8.5.

Úlohy konfigurovania

Ak chcete nakonfigurovať pripojenie pobočky opísané v tomto návrhu, musíte vykonať každú z týchto úloh:

Poznámka: Pred začatím týchto úloh si overte smerovanie TCP/IP, aby ste si boli istí, že oba systémy brán budú schopné komunikovať navzájom prostredníctvom internetu. Toto zaistí, že hostitelia na každej podsieti budú správne smerovať na svoju príslušnú bránu pre prístup na vzdialenú podsieť.

Súvisiace koncepty

Smerovanie a vyrovnávanie pracovného zaťaženia TCP/IP

Súvisiace informácie

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

Vyplnenie plánovacích pracovných listov

Plánovací kontrolný zoznam zobrazuje typy informácií, ktoré potrebujete poznať predtým, než začnete konfigurovať VPN. Skôr ako budete pokračovať v nastavovaní VPN, musia byť všetky odpovede v zozname nevyhnutných podmienok nastavené na YES.

Poznámka: Tieto pracovné listy použite na Systém A, pri Systéme C tento proces zopakujte a podľa potreby prehoďte IP adresy.

Tabuľka 1. Systémové požiadavky

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je v systém spustený i5/OS V5R3 alebo novší?	Áno
Je v ňom nainštalovaná voľba Správca digitálnych certifikátov?	Áno
Je nainštalované System i Access for Windows?	Áno
Je nainštalované System i Navigator?	Áno
Je nainštalovaný sieťový podkomponent System i Navigator?	Áno
Je nainštalované IBM TCP/IP Connectivity Utilities for i5/OS?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Máte vo vašom systéme nakonfigurované TCP/IP (vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény)?	Áno

Tabuľka 1. Systémové požiadavky (pokračovanie)

Kontrolný zoznam nevyhnutných požiadaviek	**Odpovede**
Je medzi požadovanými koncovými bodmi vytvorená normálna komunikácia TCP/IP?	Áno
Použili ste najnovšie dočasné opravy programu (PTF)?	Áno
Ak VPN tunel traverzuje firewaly alebo smerovače používajúce filtrovanie IP paketov , podporujú filtrovacie pravidlá firewalu alebo smerovača protokoly AH a ESP?	Áno
Sú firewally alebo smerovače nakonfigurované tak, aby povoľovali protokoly IKE (UDP port 500), AH a ESP?	Áno
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	Áno

Tabuľka 2. Konfigurácia VPN

Na konfiguráciu VPN budete potrebovať tieto informácie	**Odpovede**
Aký typ pripojenia vytvárate?	brána-brána
Ako pomenujete skupinu dynamických kľúčov?	HRgw2FINgw
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov?	Vyvážený
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	Bez topsecretstuff
Aký je identifikátor lokálneho servera kľúčov?	Adresa IP: 204.146.18.227
Aký je identifikátor lokálneho koncového bodu údajov?	Podsieť: 10.6.0.0 Maska: 255.255.0.0
Aký je identifikátor vzdialeného servera kľúčov?	Adresa IP: 208.222.150.250
Aký je identifikátor vzdialeného koncového bodu údajov?	Podsieť: 10.196.8.0 Maska: 255.255.255.0
Ktorým portom a protokolom chcete povoliť prenos cez pripojenie?	Všetkým
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich údajov?	Vyvážený
Na ktoré rozhrania sa pripojenie aplikuje?	TRLINE

Konfigurácia VPN v Systéme A

Dokončením týchto krokov nakonfigurujete Systém A.

Pomocou nasledujúcich krokov a informácií z vašich pracovných listov môžete nakonfigurovať VPN v Systéme A:

1. V System i Navigator rozviňte **Systém A → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Nové pripojenie.
3. Zobrazte **uvítaciu** stránku, kde nájdete informácie o objektoch, ktoré sprievodca vytvorí.
4. Kliknite na **Ďalej** a prejdite na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte HRgw2FINgw.
6. Voliteľné: Zadajte opis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdite na stránku **Scenár pripojení**.
8. Vyberte **Pripojiť vašu bránu na inú bránu**.
9. Kliknite na **Ďalej** a prejdite na stránku **Politika Internet Key Exchange**.
10. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**.
11. Kliknite na **Ďalej** a prejdite na stránku **Certifikát pre koncový bod lokálneho pripojenia**.
12. Vyberte **Nie** na označenie, že nebudete používať certifikáty na autentifikáciu pripojenia.
13. Kliknite na **Ďalej** a prejdete na stránku **Lokálny server kľúčov**.

14. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
15. V poli **adresa IP** vyberte 204.146.18.227.
16. Kliknite na **Ďalej** a prejdite na stránku **Vzdialený server kľúčov**.
17. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
18. V poli **Identifikátor** zadajte 208.222.150.250.
19. V poli **Predzdieľaný kľúč** zadajte topsecretstuff.
20. Kliknite na **Ďalej** a prejdete na stránku **Lokálny koncový bod údajov**.
21. V poli **Typ identifikátora** vyberte **Podsieť 4 verzie IP** .
22. V poli **Identifikátor** zadajte 10.6.0.0.
23. V poli **Maska podsiete** zadajte 255.255.0.0.
24. Kliknite na **Ďalej** a prejdete na stránku **Vzdialený koncový bod údajov**.
25. V poli **Typ identifikátora** vyberte **Podsieť IP verzie 4**.
26. V poli **Identifikátor** zadajte 10.196.8.0.
27. V poli **Maska podsiete** zadajte 255.255.255.0.
28. Kliknite na **Ďalej** a prejdite na stránku **Služby údajov**.
29. Použite predvolené hodnoty a potom kliknite na **Ďalej**, aby ste prešli na stránku **Politika údajov**.
30. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**.
31. Vyberte **Použiť šifrovací algoritmus RC4**.
32. Kliknite na **Ďalej** a prejdite na stránku **Použiteľné rozhrania**.
33. V tabuľke **Linka** vyberte **TRLINE**.
34. Kliknite na **Ďalej** a prejdete na stránku **Súhrn**. Prezrite objekty, ktoré vytvorí sprievodca a presvedčte sa, či sú správne.
35. Kliknutím na **Dokončiť** dokončíte konfiguráciu.
36. Keď sa objaví dialógové okno **Aktivovať filtre politík**, vyberte **Áno, aktivovať vygenerované filtre politík** a **Povoliť všetky ďalšie prenosy**.
37. Kliknutím na **OK** dokončíte konfiguráciu. Po výzve zadajte, že chcete aktivovať pravidlá na všetkých rozhraniach.

Súvisiace úlohy

"Konfigurácia VPN v Systéme C"
Postupujte podľa tých istých krokov, akými ste nakonfigurovali VPN v Systéme A, len podľa potreby zmeňte IP adresy. Použite vaše plánovacie pracovné listy na asistenciu.

Konfigurácia VPN v Systéme C

Postupujte podľa tých istých krokov, akými ste nakonfigurovali VPN v Systéme A, len podľa potreby zmeňte IP adresy. Použite vaše plánovacie pracovné listy na asistenciu.

Po dokončení konfigurácie VPN brán finančného oddelenia budú vaše pripojenia v stave *na požiadanie*, ktorý znamená, že pripojenie sa aktivuje vtedy, keď sa odošlú IP datagramy, ktoré musí toto pripojenie VPN ochraňovať. Ďalším krokom bude spustenie serverov VPN, v prípade, že už nie sú spustené.

Súvisiace úlohy

"Konfigurácia VPN v Systéme A" na strane 15
Dokončením týchto krokov nakonfigurujete Systém A.

Spustenie VPN

Ak ste už vaše pripojenie VPN v Systémoch A a C nakonfigurovali, potrebujete toto pripojenie VPN spustiť.

VPN spustíte nasledujúcim postupom:

1. V System i Navigator rozviňte položku **systém → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a zvoľte **Spustiť**.

Testovanie pripojenia

Po dokončení konfigurácie oboch systémov a po úspešnom spustení serverov VPN otestujte ich pripojiteľnosť, aby ste sa overili, či môžu vzdialené podsiete navzájom komunikovať.

Pri testovaní vášho pripojenia postupujte podľa týchto krokov:

1. V System i Navigator rozviňte **Systém A → Sieť**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia TCP/IP**, vyberte **Nástroje** a potom **Ping**.
3. V dialógovom okne **Ping from** v poli **Ping** zadajte Systém C.
4. Kliknutím na **Ping Now** overte pripojiteľnosť zo Systému A na Systém C.
5. Po dokončení kliknite na **OK**.

Návrh: Základné medzipodnikové pripojenie

V tomto návrhu chce vaša spoločnosť vytvoriť VPN medzi klientskou pracovnou stanicou vo vašej výrobnej divízii a klientskou pracovnou stanicou v oddelení dodávok vášho obchodného partnera.

Situácia

Veľa spoločností používa na zabezpečenie komunikácie s ich obchodnými partnermi, dcérskymi spoločnosťami a predajcami frame relay alebo prenajaté linky. Nanešťastie sú tieto riešenia často drahé a existujú pre ne geografické obmedzenia. VPN poskytuje alternatívu pre firmy, ktoré potrebujú využívať privátnu a na náklady nenáročnú komunikáciu.

Predpokladajme, že ste hlavný dodávateľ súčiastok pre nejakého výrobcu. Keďže je rozhodujúce, aby ste mali určité súčiastky a množstvá k dispozícii presne v určenom čase podľa požiadaviek podniku výrobcu, musíte byť neustále informovaní o stave inventára a výrobných plánoch výrobcu. Možno túto interakciu v súčasnosti zvládnete manuálne a zistíte, že je časovo náročná, nákladná a rovnako aj časovo nepresná. Chcete na komunikáciu s vašou výrobnou spoločnosťou nájsť lahší, rýchlejší a účinnejší spôsob. Ale keďže treba vziať do úvahy dôvernosť a časovú háklivosť informácií, ktoré si vymieňate, výrobca nebude chcieť publikovať ich na svojej firemnej webovej stránke alebo ich distribuovať každý mesiac v externej správe. Využitím verejného internetu môžete jednoducho vytvoriť VPN, ktorá bude vyhovovať potrebám oboch spoločností.

Ciele

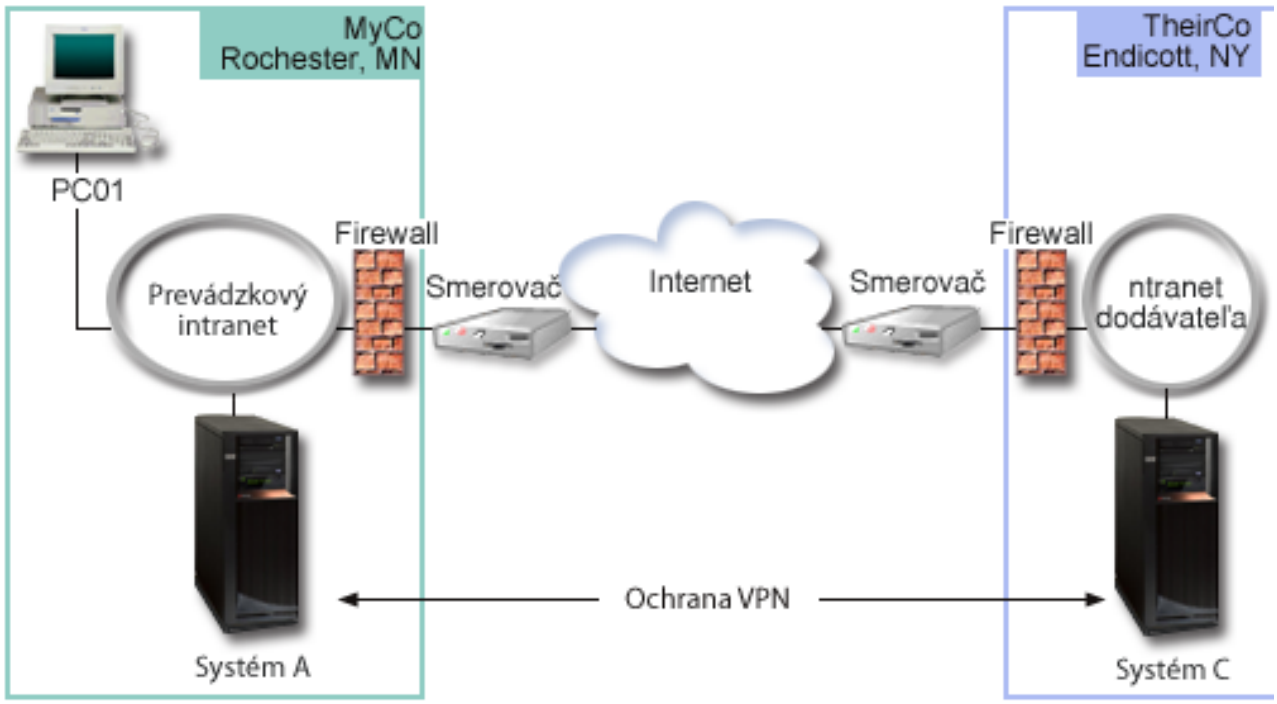
V tomto návrhu chce spoločnosť MyCo vytvoriť VPN medzi hostiteľom vo svojej divízii súčiastok a hostiteľom vo výrobnom oddelení jedného zo svojich obchodných spoločníkov, TheirCo.

Keďže informácie, ktoré zdieľajú tieto dve spoločnosti, sú vysoko dôverné, počas svojho pohybu po internete musia byť chránené. Údaje sa navyše nesmú v rámci žiadnej podnikovej siete prenášať v nezašifrovanej forme, pretože každá sieť považuje druhú sieť za nedôveryhodnú. Inými slovami, obe spoločnosti vyžadujú autentifikáciu, integritu a šifrovanie na úrovni koncového zariadenia.

Dôležité: Zámerom tohto návrhu je príkladom predložiť jednoduchú konfiguráciu VPN typu hostiteľ-hostiteľ. V typickom sieťovom prostredí budete tiež musieť uvažovať o konfigurácii firewallu, požiadavkách adresovania IP a medzi iným aj smerovaní.

Detaily

Nasledujúci obrázok ilustruje charakteristiky siete spoločnosti MyCo a TheirCo.



Sieť dodávateľskej spoločnosti MyCo

- Systém A je spustený na i5/OS verzia 5 vydanie 3 (V5R3) alebo novšia.
- IP adresa Systému A je 10.6.1.1. Toto je koncový bod pripojenia, ako aj koncový bod údajov. To znamená, že Systém A vykonáva vyjednávania IKE a na prichádzajúce a odchádzajúce datagramy využíva protokol IPSec a zároveň je zdrojom a cieľom údajom prenášaných prostredníctvom VPN.
- Systém A je v podsieti 10.6.0.0 s maskou 255.255.0.0.
- Pripojenie k Systému C môže iniciovať len Systém A.

Sieť výrobnej spoločnosti TheirCo

- Systém C je spustený na i5/OS verzia 5 vydanie 3 (V5R3) alebo novšia.
- IP adresa Systému C je 10.196.8.6. Toto je koncový bod pripojenia, ako aj koncový bod údajov. To znamená, že Systém A vykonáva vyjednávania IKE a na prichádzajúce a odchádzajúce datagramy využíva protokol IPSec a zároveň je zdrojom a cieľom údajom prenášaných prostredníctvom VPN.
- Systém C je v podsieti 10.196.8.0 s maskou 255.255.255.0.

Úlohy konfigurovania

Ak chcete nakonfigurovať medzipodnikové pripojenie popísané v tomto návrhu, musíte vykonať každú z týchto úloh:

Poznámka: Pred začatím týchto úloh si overte smerovanie TCP/IP, aby ste si boli istí, že oba systémy brán budú schopné komunikovať navzájom prostredníctvom internetu. Toto zaistí, že hostitelia na každej podsieti budú správne smerovať na svoju príslušnú bránu pre prístup na vzdialenú podsieť.

Súvisiace koncepty

Smerovanie a vyrovnávanie pracovného zaťaženia TCP/IP

Vyplnenie plánovacích pracovných listov

Plánovací kontrolný zoznam zobrazuje typy informácií, ktoré potrebujete poznať predtým, než začnete konfigurovať VPN. Skôr ako budete pokračovať v nastavovaní VPN, musia byť všetky odpovede v zozname nevyhnutných podmienok nastavené na YES.

Poznámka: Tieto pracovné listy použite na Systém A, pri Systéme C tento proces zopakujte a podľa potreby prehoďte IP adresy.

Tabuľka 3. Systémové požiadavky

Kontrolný zoznam nevyhnutných požiadaviek	**Odpovede**
Je v systém spustený i5/OS V5R3 alebo novší?	Áno
Je v ňom nainštalovaná voľba Správca digitálnych certifikátov?	Áno
Je nainštalované System i Access for Windows?	Áno
Je nainštalované System i Navigator?	Áno
Je nainštalovaný sieťový podkomponent System i Navigator?	Áno
Je nainštalované IBM TCP/IP Connectivity Utilities for i5/OS?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Máte vo vašom systéme nakonfigurované TCP/IP (vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény)?	Áno
Je medzi požadovanými koncovými bodmi vytvorená normálna komunikácia TCP/IP?	Áno
Použili ste najnovšie dočasné opravy programu (PTF)?	Áno
Ak VPN tunel traverzuje firewaly alebo smerovače používajúce filtrovanie IP paketov , podporujú filtrovacie pravidlá firewalu alebo smerovača protokoly AH a ESP?	Áno
Sú firewally alebo smerovače nakonfigurované tak, aby povoľovali protokoly IKE (UDP port 500), AH a ESP?	Áno
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	Áno

Tabuľka 4. Konfigurácia VPN

Na konfiguráciu VPN budete potrebovať tieto informácie	**Odpovede**
Aký typ pripojenia vytvárate?	brána-brána
Ako pomenujete skupinu dynamických kľúčov?	HRgw2FINgw
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov?	Vyvážený
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	Bez topsecretstuff
Aký je identifikátor lokálneho servera kľúčov?	Adresa IP: 204.146.18.227
Aký je identifikátor lokálneho koncového bodu údajov?	Podsieť: 10.6.0.0 Maska: 255.255.0.0
Aký je identifikátor vzdialeného servera kľúčov?	Adresa IP: 208.222.150.250
Aký je identifikátor vzdialeného koncového bodu údajov?	Podsieť: 10.196.8.0 Maska: 255.255.255.0
Ktorým portom a protokolom chcete povoliť prenos cez pripojenie?	Všetkým
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich údajov?	Vyvážený
Na ktoré rozhrania sa pripojenie aplikuje?	TRLINE

Konfigurácia VPN v Systéme A

Dokončením nasledujúcich krokov môžete nakonfigurovať pripojenie VPN v Systéme A.

Pri konfigurácii VPN v Systéme A použite nasledujúcim spôsobom informácie z vašich plánovacích pracovných listov:

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Pripojenie.
3. Zobrazte **uvítaciu** stránku, kde nájdete informácie o objektoch, ktoré sprievodca vytvorí.
4. Kliknite na **Ďalej** a prejdite na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte MyCo-TheirCo.
6. Voliteľné: Zadajte opis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdite na stránku **Scenár pripojení**.
8. Vyberte **Pripojiť vášho hostiteľa na iného hostiteľa**.
9. Kliknite na **Ďalej** a prejdite na stránku **Politika Internet Key Exchange**.
10. Vyberte **Vytvoriť novú politiku** a potom vyberte **Najvyššia bezpečnosť, najnižší výkon**.
11. Kliknite na **Ďalej** a prejdite na stránku **Certifikát pre koncový bod lokálneho pripojenia**.
12. Vyberte **Áno** na označenie, že budete používať certifikáty na autentifikáciu pripojenia. Potom vyberte certifikát, ktorý predstavuje Systém A.

    Poznámka: Ak chcete použiť certifikát na autentifikáciu koncového bodu lokálneho pripojenia, najprv vytvorte tento certifikát v Správcovi digitálnych certifikátov (DCM).
13. Kliknite na **Ďalej** a prejdete na stránku **Identifikátor lokálneho koncového bodu pripojenia**.
14. Ako typ identifikátora vyberte **Adresa IP verzie 4**. Priradená IP adresa musí byť 10.6.1.1. Rovnako, tieto informácie sú definované v certifikáte, ktorý vytvoríte v DCM.
15. Kliknite na **Ďalej** a prejdite na stránku **Vzdialený server kľúčov**.
16. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
17. V poli **Identifikátor** zadajte 10.196.8.6.
18. Kliknite na **Ďalej** a prejdite na stránku **Služby údajov**.
19. Použite predvolené hodnoty a potom kliknite na **Ďalej**, aby ste prešli na stránku **Politika údajov**.
20. Vyberte **Vytvoriť novú politiku** a potom vyberte **Najvyššia bezpečnosť, najnižší výkon**. Vyberte **Použiť šifrovací algoritmus RC4**.
21. Kliknite na **Ďalej** a prejdite na stránku **Použiteľné rozhrania**.
22. Vyberte **TRLINE**.
23. Kliknite na **Ďalej** a prejdete na stránku **Súhrn**. Prezrite objekty, ktoré vytvorí sprievodca a presvedčte sa, či sú správne.
24. Kliknutím na **Dokončiť** dokončíte konfiguráciu.
25. Keď sa objaví dialógové okno **Aktivovať filtre politík**, vyberte **Nie, pravidlá pre pakety budú aktivované neskôr** a kliknite na **OK**.

Nasledujúcim krokom stanovíte, že toto pripojenie môže iniciovať jedine Systém A. Vykonáte ho prispôsobením vlastností skupiny dynamických kľúčov, MyCo-TheirCo, ktorú vytvoril sprievodca:

1. V ľavom okne rozhrania VPN kliknite na **Podľa skupiny**, v pravom okne sa zobrazí nová skupina dynamických kľúčov MyCo-TheirCo. Kliknite na ňu pravým tlačidlom a vyberte **Vlastnosti**.
2. Prejdite na stránku **Politika** a vyberte voľbu **Lokálny systém zahájí pripojenie**.
3. Kliknutím na **OK** uložíte vaše zmeny.

Konfigurácia VPN v Systéme C

Postupujte podľa tých istých krokov, akými ste nakonfigurovali VPN v Systéme A, len podľa potreby zmeňte IP adresy. Použite vaše plánovacie pracovné listy na asistenciu.

Po dokončení konfigurácie VPN brán finančného oddelenia budú vaše pripojenia v stave *na požiadanie*, ktorý znamená, že pripojenie sa aktivuje vtedy, keď sa odošlú IP datagramy, ktoré musí toto pripojenie VPN ochraňovať. Ďalším krokom bude spustenie serverov VPN, v prípade, že už nie sú spustené.

Aktivácia pravidiel pre pakety

Sprievodca VPN automatický vytvorí pravidlá pre pakety, ktoré sú nevyhnutné pre správne fungovanie tohto pripojenia. Ale než budete môcť spustiť pripojenie VPN, musíte ich aktivovať na oboch systémoch.

Pri aktivácii pravidiel pre pakety v Systéme A postupujte podľa týchto krokov:

1. V System i Navigator rozviňte **Systém A → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Aktivovať**. Toto otvorí dialógové okno **Aktivovať pravidlá pre pakety**.
3. Vyberte, či chcete aktivovať len vygenerované pravidlá VPN, len vybraný súbor alebo aj vygenerované pravidlá VPN aj vybraný súbor. Druhú možnosť môžete vybrať, ak napríklad máte rôznorodé pravidlá PERMIT a DENY, ktoré chcete vynútiť na rozhraní okrem vygenerovaných pravidiel VPN.
4. Vyberte rozhranie, na ktorom chcete aktivovať pravidlá. V tomto prípade vyberte **Všetky rozhrania**.
5. V dialógovom okne kliknite na **OK**, čím potvrdíte, že si želáte overiť a aktivovať pravidlá na zadaných rozhraniach. Keď kliknete na OK, systém skontroluje pravidlá pre syntaktické a sémantické chyby ohlási výsledky v okne správy v spodnej časti editora. Chybové správy, ktoré sú spojené s určitým súborom a číslom riadka, získate, keď kliknete pravým tlačidlom na chybu a vyberiete **Prejsť na riadok**, čím zvýrazníte chybu v súbore.
6. Zopakovaním týchto krokov aktivujte aj pravidlá pre pakety v Systéme C.

Spustenie pripojenia

Ak ste už vaše pripojenie VPN nakonfigurovali, potrebujete toto pripojenie VPN spustiť.

Ak chcete spustiť pripojenie MyCo2TheirCo zo Systému A, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte **Systém A → Network → IP Policies**.
2. Ak nie je server VPN spustený, kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Spustiť**. Takto spustíte server VPN.
3. Rozviňte **Budovanie VPN → Bezpečné pripojenia**.
4. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
5. Kliknite pravým tlačidlom na **MyCo-TheirCo** a vyberte **Spustiť**.
6. Z ponuky **Zobrazenie** vyberte **Obnoviť**. Ak je pripojenie úspešne spustené, stav sa zmení z *Nečinný* na *Povolený*. Spúšťanie pripojenia môže trvať niekoľko minút, preto pravidelne obnovujte okno, až kým sa jeho stav nezmení na *Povolený*.

Testovanie pripojenia

Po dokončení konfigurácie oboch systémov a po úspešnom spustení serverov VPN otestujte ich pripojiteľnosť, aby ste sa overili, či môžu vzdialené podsiete navzájom komunikovať.

Pri testovaní vášho pripojenia postupujte podľa týchto krokov:

1. V System i Navigator rozviňte **Systém A → Sieť**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia TCP/IP**, vyberte **Nástroje** a potom **Ping**.
3. V dialógovom okne **Ping from** v poli **Ping** zadajte Systém C.
4. Kliknutím na **Ping Now** overte pripojiteľnosť zo Systému A na Systém C.
5. Po dokončení kliknite na **OK**.

Scenár: Ochrana dobrovoľného tunela L2TP protokolom IPSec

V tomto scenári sa oboznámite so spôsobom nastavenia pripojenia medzi kancelárskym hostiteľom pobočky a centrály, ktoré používa L2TP chránené pomocou IPSec. Pobočka má dynamicky priradenú adresu IP, zatiaľ čo centrála spoločnosti má statickú, globálne smerovateľnú adresu IP.

Situácia

Predpokladajme, že vaša spoločnosť má malú pobočku v inom štáte. Počas ktoréhokoľvek pracovného dňa môže pobočka spoločnosti vyžadovať prístup k utajeným informáciám o modeli System i vo vašom podnikovom intranete. Vaša spoločnosť v súčasnosti používa na zabezpečenie prístupu pobočky do podnikovej siete drahú prenajatú linku. Hoci vaša spoločnosť chce aj naďalej poskytovať bezpečný prístup k svojmu intranetu, nakoniec chcete znížiť náklady vynakladané na prenajatú linku. To môžete uskutočniť tak, že vytvoríte dobrovoľný tunel Tunelový protokol vrstvy 2 (L2TP), ktorý rozšíri vašu podnikovú sieť, takže vaša pobočka sa bude vystupovať ako súčasť vašej podnikovej podsiete. VPN ochraňuje prenos údajov cez tunel L2TP.

S dobrovoľným tunelom L2TP vytvorí vzdialená pobočka tunel priamo na sieťový server L2TP (L2TP network server, LNS) podnikovej siete. Funkčnosť koncentrátora prístupu L2TP (access concentrator L2TP, LAC) spočíva na klientovi. Tunel je pre Poskytovateľa internetových služieb (ISP) klienta transparentný, takže na podporu L2TP sa nevyžaduje ISP. Ak chcete získať viac informácií o konceptoch L2TP, pozrite si protokol L2TP (Layer 2 Tunnel Protocol).

Dôležité: Tento scenár zobrazuje bezpečnostné brány, ktoré sú priamo pripojené k Internetu. Nie je tu firewall kvôli zjednodušeniu návrhu. Neznamená to, že použitie firewallu nie je nevyhnutné. Zvážte bezpečnostné riziká, ktorým sa vystavujete pri každom pripojení na internet.

Ciele

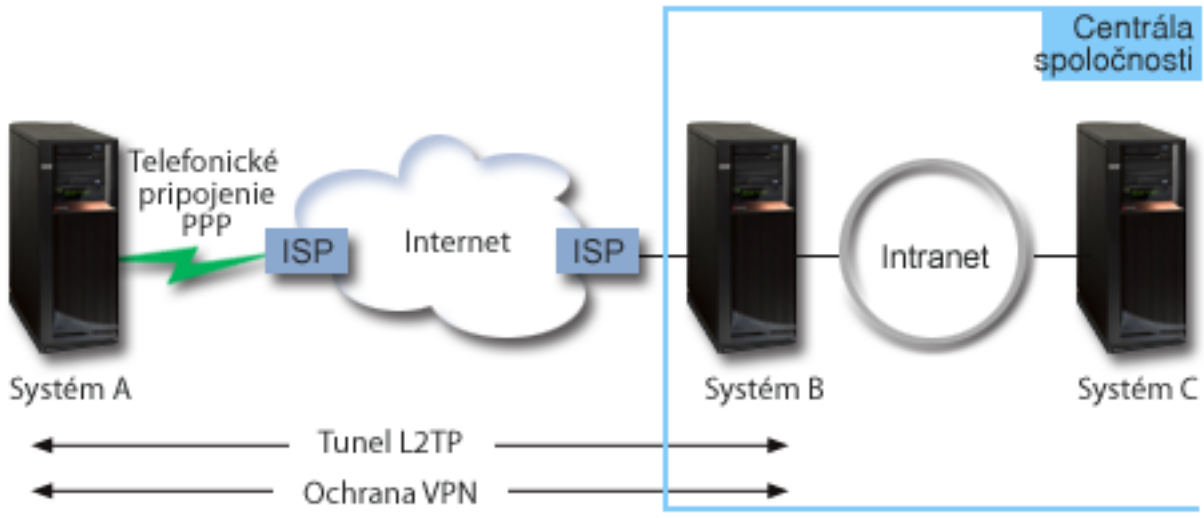
V tomto scenári sa kancelársky systém pobočky pripojí k svojej firemnej sieti cez systém brány pomocou tunela L2TP chráneného pomocou VPN.

Hlavnými cieľmi tohto návrhu sú:

- Systém pobočky vždy zahajuje pripojenie na podnikovú ústredňu.
- Systém pobočky je jediným systémom v sieti pobočky, ktorý potrebuje prístup na podnikovú sieť. Inými slovami, jeho rola v sieti pobočky je hostiteľ, nie brána.
- Podnikový systém hostiteľský počítač v sieti pobočky.

Detaily

Nasledujúci obrázok ilustruje charakteristiky siete pre tento návrh.



Systém A

- Musí mať prístup k aplikáciám TCP/IP vo všetkých systémoch vo firemnej sieti.

- Prijíma dynamicky priradené adresy IP od svojho ISP.
- Musí byť nakonfigurovaný na poskytovanie podpory L2TP.

Systém B

- Musí mať prístup k aplikáciám TCP/IP v Systéme A.
- Podsieť je 10.6.0.0 s maskou 255.255.0.0. Táto podsieť reprezentuje koncový bod údajov tunela VPN na podnikovej lokalite.
- Pripája sa na Internet s adresou IP 205.13.237.6. Toto je koncový bod pripojenia. To znamená, že Systém B vykonáva riadenie kľúčov a na prichádzajúce a odchádzajúce datagramy používa protokol IPSec. Systém B je k svojej podsieti pripojený s IP adresou 10.6.11.1.

Z hľadiska L2TP *Systém A* vystupuje ako iniciátor L2TP, zatiaľ čo *Systém B* vystupuje ako terminátor L2TP.

Úlohy konfigurovania

Za predpokladu, že konfigurácia TCP/IP už existuje a funguje, musíte vykonať nasledujúce úlohy:

Súvisiace koncepty

"Protokol L2TP (Layer 2 Tunnel Protocol)" na strane 7
Pripojenia L2TP (Layer 2 Tunneling Protocol), nazývané aj virtuálne linky, umožňujú, aby podnikové sieťové systémy riadili IP adresy priradené vzdialeným užívateľom, vďaka čomu týmto vzdialeným užívateľom poskytujú cenovo výhodný prístup. Okrem toho pripojenia L2TP poskytujú bezpečný prístup do vášho systému alebo siete, keď ich používate v spojení s Bezpečnosťou IP (IPSec)

Súvisiace informácie

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

Konfigurácia VPN v Systéme A

Dokončením nasledujúcich krokov môžete nakonfigurovať pripojenie VPN v Systéme A.

Pri konfigurácii VPN v Systéme A použite nasledujúcim spôsobom informácie z vašich plánovacích pracovných listov:

1. **Nakonfigurovať politiku Internet Key Exchange**
   a. V System i Navigator rozviňte Systém A → **Sieť** → **Politiky IP** → **Virtuálne súkromné siete** → **Politiky bezpečnosti IP**.
   b. Pravým tlačidlom myši kliknite na **Politiky Internet Key Exchange** a vyberte **Nová politika Internet Key Exchange**.
   c. Na stránke **Vzdialený server** vyberte **Adresa IP verzie 4** ako identifikátor typu a potom v poli **Adresa IP** zadajte 205.13.237.6.
   d. Na stránke **Asociácie** vyberte **Dopredu zdieľaný kľúč** na označenie, že toto pripojenie na autentifikáciu tejto politiky používa dopredu zdieľaný kľúč.
   e. V poli **Kľúč** zadajte dopredu zdieľaný kľúč. Ako heslo použite váš dopredu zdieľaný kľúč.
   f. Vyberte **Identifikátor kľúča** pre typ identifikátora lokálneho servera kľúčov a v poli **Identifikátor** zadajte identifikátor kľúča. Napríklad thisisthekeyid. Nezabudnite, že lokálny server kľúčov má dynamický priradenú adresu IP, ktorú nemožno vedieť dopredu. Keď Systém A iniciuje pripojenie, identifikuje ho Systém B pomocou tohto identifikátora.
   g. Kliknutím na **Add** na stránke **Transforms** pridáte zmeny, ktoré Systém A kvôli ochrane kľúča navrhuje Systému B a stanovíte, či má pri iniciácii prvej fázy vyjednávania politika IKE využívať ochranu identity.
   h. Na stránke **Transformácia politiky IKE** vyberte **Dopredu zdieľaný kľúč** pre vašu autentifikačnú metódu, **SHA** pre váš transformačný algoritmus a **3DES-CBC** pre váš šifrovací algoritmus. Prijmite predvolené hodnoty pre skupinu Diffie-Hellmana a Ukončiť platnosť kľúčov IKE po.
   i. Kliknite na **OK** a vrátite sa na stránku **Transformácie**.
   j. Vyberte **Agresívny režim dohodovania IKE (bez ochrany identity).**

Poznámka: Ak používate predzdieľané kľúče aj agresívny režim dohodovania vo vašej konfigurácii, vyberte skrytie hesiel, ktoré takto nebude jednoduché odhaliť pri útoku skenovaním slovníka. Taktiež sa odporúča, aby ste si pravidelne menili svoje heslá.

k. Kliknite na **OK** a vaše konfigurácie sa uložia.

2. **Nakonfigurovať údajovú politiku**
   a. V rozhraní VPN pravým tlačidlom myši kliknite na **Politiky údajov** a vyberte **Nová politika údajov**
   b. Na stránke **Všeobecné** zadajte názov údajovej politiky. Napríklad l2tpremoteuser.
   c. Prejdite na stránku **Návrhy**. Návrh je zbierka protokolov, ktorú používajú zahajujúce a odpovedajúce severy kľúčov na vytvorenie dynamického pripojenia medzi dvomi koncovými bodmi. Jednu údajovú politiku môžete použiť v niekoľkých objektoch pripojenia. Ale nie všetky vzdialené VPN servery kľúčov nevyhnutne majú rovnaké vlastnosti údajovej politiky. Preto môžete do jednej údajovej politiky pridať niekoľko návrhov. Keď vytvárate pripojenie VPN na vzdialený server kľúčov, v údajovej politike musí existovať minimálne jeden zhodný návrh iniciátora a respondenta.
   d. Kliknite na **Pridať**, aby ste pridali transformáciu politiky údajov.
   e. Vyberte **Prenos** pre režim zapuzdrenia.
   f. Kliknite na **OK** a vrátite sa na stránku **Transformácie**.
   g. Zadajte hodnotu pre ukončenie platnosti kľúča.
   h. Kliknite na **OK** a vaša nová údajová politika sa uloží.
3. **Nakonfigurovať skupinu dynamických kľúčov**
   a. V rozhraní VPN rozviňte **Bezpečné pripojenia**.
   b. Pravým tlačidlom myši kliknite na **Podľa skupiny** a vyberte **Nová skupina dynamických kľúčov**.
   c. Na stránke **Všeobecné** zadajte názov množiny pre skupinu. Napríklad l2tptocorp.
   d. Vyberte **Ochraňuje lokálne inicializovaný tunel L2TP**.
   e. Pre rolu systému vyberte **Oba systémy sú hostitelia**.
   f. Prejdite na stránku **Politika**. Zo sťahovacieho zoznamu **Politika údajov** vyberte politiku údajov, ktorú ste vytvorili v kroku **Konfigurovať politiku údajov**, l2tpremoteuser.
   g. Vyberte **Local system initiates connection** , čím určíte, že toto spojenie so Systémom B môže iniciovať len Systém A.
   h. Prejdite na stránku **Pripojenia**. Vyberte **Vygenerovať nasledujúce pravidlo pre filtre politiky pre túto skupinu**. Kliknite na **Úpravy** a definujte parametre filtra politiky.
   i. Na stránke **Filter politiky- Lokálne adresy** vyberte **Identifikátor kľúča** pre typ identifikátora.
   j. Pre identifikátor vyberte identifikátor kľúča totojeidkluca, ktorý ste definovali v politike IKE.
   k. Prejdite na stránku **Filter politiky - Vzdialené adresy**. V rozbaľovacom zozname **Typ identifikátora** vyberte **Adresa IP verzie 4**.
   l. V poli **Identifikátor** zadajte 205.13.237.6.
   m. Prejdite na stránku **Filter politiky - Služby**. V poliach **Lokálny port** a **Vzdialený port** zadajte 1701. Port 1701 je známy port pre L2TP.
   n. V rozbaľovacom zozname **Protokol** vyberte **UDP**.
   o. Kliknite na **OK** a vrátite sa na stránku **Pripojenia**.
   p. Prejdite na stránku **Rozhrania**. Vyberte ktorúkoľvek linku alebo profil PPP, na ktorý sa táto skupina použije. Ešte ste nevytvorili profil PPP pre túto skupinu. Keď to vykonáte, budete musieť upraviť vlastnosti tejto skupiny, aby sa skupina použila na profil PPP, ktorý vytvoríte v ďalšom kroku.
   q. Kliknutím na **OK** vytvoríte skupinu dynamických kľúčov, l2tptocorp.
4. **Nakonfigurovať pripojenie dynamických kľúčov**
   a. V rozhraní VPN rozviňte **Podľa skupiny**. Tým zobrazíte zoznam všetkých skupín dynamických kľúčov, ktoré ste pre Systém A nakonfigurovali.
   b. Kliknite pravým tlačidlom na **14tpnapodnik** a vyberte **Nové pripojenie dynamických kľúčov**.
   c. Na stránke **Všeobecné** zadajte voliteľný popis pre pripojenie.

d. Pre vzdialený server kľúčov vyberte **Adresa IP verzie 4** pre typ identifikátora.
e. V rozbaľovacom zozname Adresa IP vyberte **205.13.237.6**.
f. Zrušte výber **Spustiť na požiadanie**.
g. Prejdite na stránku **Lokálne adresy**. Vyberte **Identifikátor kľúča** pre typ identifikátora a z rozbaľovacieho zoznamu **Identifikátor** vyberte totojeidkluca.
h. Prejdite na stránku **Vzdialené adresy**. Vyberte **Adresa IP verzie 4** pre typ identifikátora.
i. V poli **Identifikátor** zadajte 205.13.237.6.
j. Prejdite na stránku **Služby**. V poliach **Lokálny port** a **Vzdialený port** zadajte 1701. Port 1701 je známy port pre L2TP.
k. Zo sťahovacieho zoznamu **Protokol** vyberte **UDP**.
l. Kliknutím na **OK** vytvoríte pripojenie dynamických kľúčov.

Súvisiace úlohy

"Konfigurácia VPN v Systéme B" na strane 26
Pri konfigurácii pripojenia VPN v Systéme B postupuje podľa tých istých krokov, aké ste použili počas konfigurácie pripojenia VPN v Systéme A, len podľa potreby zmeňte IP adresy a identifikátory.

Konfigurácia profilu PPP a virtuálnej linky v Systém A

Keď už máte v Systéme A nakonfigurované pripojenie VPN, potrebujete v tomto systéme vytvoriť profil PPP. Profilu PPP nie je priradená žiadna fyzická linka, namiesto toho využíva virtuálnu linku. To preto, lebo prenos PPP prechádza tunelom L2TP, zatiaľ čo VPN ochraňuje tunel L2TP.

Pri vytvorení profilu pripojenia PPP v Systéme A postupujte podľa týchto krokov:

1. V System i Navigator rozviňte Systém A → **Sieť** → **Služby vzdialeného prístupu**.
2. Kliknite pravým tlačidlom na **Profily pripojenia pôvodcu** a vyberte **Nový profil**.
3. Na stránke **Nastavenie** vyberte **PPP** pre typ protokolu.
4. Pri výberoch Režim vyberte **L2TP (virtuálna linka)**.
5. Z rozbaľovacieho zoznamu **Režim činnosti** vyberte **Iniciátor na požiadanie (dobrovoľný tunel)**.
6. Kliknite na **OK** a prejdete na stránku vlastností profilov PPP.
7. Na stránke **Všeobecné** zadajte názov, ktorý identifikuje typ a cieľ pripojenia. V tomto prípade zadajte toCORP. Názov, ktorý zadáte, musí mať 10 alebo menej znakov.
8. Voliteľné: zadajte opis pre profil.
9. Prejdite na stránku **Pripojenie**.
10. V poli **Názov virtuálnej linky** z rozbaľovacieho zoznamu vyberte **tocorp**. Nezabudnite, že táto linka nemá priradené žiadne fyzické rozhranie. Virtuálna linka popisuje rôzne charakteristiky profilu PPP. Napríklad maximálnu veľkosť rámikov, autentifikačné informácie, názov lokálneho hostiteľa atď. Otvorí sa dialógové okno **Vlastnosti linky L2TP**.
11. Na stránke **Všeobecné** zadajte popis pre virtuálnu linku.
12. Prejdite na stránku **Autentifikácia**.
13. V poli **Local host name** zadajte názov hostiteľa lokálneho servera kľúčov, SystemA.
14. Kliknutím na **OK** uložíte popis novej virtuálnej linky a vrátite sa na stránku **Pripojenie**.
15. V poli **Adresa koncového bodu vzdialeného tunela** zadajte adresu koncového bodu vzdialeného tunela, 205.13.237.6.
16. Vyberte **Vyžaduje ochranu IPSec** a vyberte skupinu dynamických kľúčov, ktorú ste vytvorili v predošlom kroku "Konfigurácia VPN v Systéme A" na strane 23, l2tptocorp zo sťahovacieho zoznamu **Názov skupiny pripojení**.
17. Prejdite na stránku **Nastavenia TCP/IP**.
18. V časti **Lokálna adresa IP** vyberte **Priradená vzdialeným systémom**.
19. V časti **Vzdialená adresa IP** vyberte **Použiť pevnú adresu IP**. Zadajte 10.6.11.1, čo je adresa IP vzdialeného systému v jeho podsieti.

20. V smerovacej časti vyberte **Definovať ďalšie trasy** a kliknite na **Trasy**. Ak nie sú v profile PPP zadané žiadne informácie o smerovaní, bude Systém A schopný dosiahnuť len koncový bod vzdialeného tunela a nedosiahne na žiaden iný systém v podsieti 10.6.0.0.
21. Kliknite na **Pridať** a pridáte položku statickej trasy.
22. Zadajte podsieť 10.6.0.0 a masku podsiete 255.255.0.0 na smerovanie celého prenosu 10.6.*.* cez tunel L2TP.
23. Kliknite na **OK** a pridáte statickú trasu.
24. Zatvorte dialógové okno smerovania kliknutím na **OK**.
25. Prejdite na stránku **Autentifikácia** a nastavte meno užívateľa a heslo pre tento profil PPP.
26. V časti Identifikácia lokálneho systému vyberte **Povoliť vzdialenému systému overovať totožnosť tohto systému**.
27. V časti **Autentifikačný protokol na použitie** vyberte **Vyžadovať zašifrované heslo (CHAP-MD5)**. V časti Identifikácia lokálneho systému vyberte **Povoliť vzdialenému systému overovať totožnosť tohto systému**.
28. Zadajte meno užívateľa, SystemA a heslo.
29. Kliknite na **OK** a uložíte profil PPP.

Použitie skupiny dynamických kľúčov l2tptocorp v profile PPP toCorp

Keď ste nakonfigurovali profil pripojenia PPP, musíte prejsť späť ku skupine dynamických kľúčov, l2tptocorp, ktorú ste vytvorili a priradiť ju k profilu PPP.

Pri priradení vašej skupiny dynamických kľúčov profilu PPP postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections → By Group**.
2. Kliknite pravým tlačidlom na skupinu dynamických kľúčov, l2tptocorp, a vyberte **Vlastnosti**.
3. Prejdite na stranu **Rozhrania** a vyberte **Použiť túto skupinu** na profil PPP, ktorý ste vytvorili v “Konfigurácia profilu PPP a virtuálnej linky v Systém A” na strane 25, toCorp.
4. Kliknutím na **OK** použijete l2tptocorp na profil PPP, toCorp.

Konfigurácia VPN v Systéme B

Pri konfigurácii pripojenia VPN v Systéme B postupuje podľa tých istých krokov, aké ste použili počas konfigurácie pripojenia VPN v Systéme A, len podľa potreby zmeňte IP adresy a identifikátory.

Kým začnete vezmite do úvahy tieto ďalšie body:

- Identifikujte vzdialený server kľúčov podľa identifikátora kľúča, ktorý ste zadali pre lokálny server kľúčov v Systéme A. Napríklad thisisthekeyid.
- Použite *presne* tie isté dopredu zdieľané kľúče.
- Overte si, že sú tu zadané transformácie zhodné s transformáciami, ktoré ste nakonfigurovali v Systéme A, inak dôjde k zlyhaniu pripojenia.
- Nezadávajte **Ochráni lokálne inicializovaný tunel L2TP** na stránke **Všeobecné** skupiny dynamických kľúčov.
- Vzdialený systém zahajuje pripojenie.
- Určite, že pripojenie by sa malo spustiť na požiadanie.

Súvisiace úlohy

“Konfigurácia VPN v Systéme A” na strane 23
Dokončením nasledujúcich krokov môžete nakonfigurovať pripojenie VPN v Systéme A.

Konfigurácia profilu PPP a virtuálnej linky v Systém B

Keď už máte v Systéme B nakonfigurované pripojenie VPN, potrebujete v tomto systéme vytvoriť profil PPP. Profilu PPP nie je priradená žiadna fyzická linka, namiesto fyzickej využíva virtuálnu linku. To preto, lebo prenos PPP prechádza tunelom L2TP, zatiaľ čo VPN ochraňuje tunel L2TP.

Pri vytvorení profilu pripojenia PPP v Systéme B postupujte podľa týchto krokov:

1. V System i Navigator rozviňte Systém B → **Sieť → Služby vzdialeného prístupu**.

2. Kliknite pravým tlačidlom na **Profily pripojenia respondenta** a vyberte **Nový profil**.
3. Na stránke **Nastavenie** vyberte **PPP** pre typ protokolu.
4. Pri výberoch Režim vyberte **L2TP (virtuálna linka)**.
5. Z rozbaľovacieho zoznamu **Režim činnosti** vyberte **Terminátor (sieťový server)**.
6. Na stránke vlastností profilov PPP kliknite na **OK**.
7. Na stránke **Všeobecné** zadajte názov, ktorý identifikuje typ a cieľ pripojenia. V tomto prípade zadajte tobranch. Názov, ktorý zadáte, musí mať 10 alebo menej znakov.
8. Voliteľné: zadajte opis pre profil.
9. Prejdite na stránku **Pripojenie**.
10. Vyberte adresu IP koncového bodu lokálneho tunela, 205.13.237.6.
11. V poli **Názov virtuálnej linky** z rozbaľovacieho zoznamu vyberte **tobranch**. Nezabudnite, že táto linka nemá priradené žiadne fyzické rozhranie. Virtuálna linka popisuje rôzne charakteristiky profilu PPP. Napríklad maximálnu veľkosť rámikov, autentifikačné informácie, názov lokálneho hostiteľa atď. Otvorí sa dialógové okno **Vlastnosti linky L2TP**.
12. Na stránke **Všeobecné** zadajte popis pre virtuálnu linku.
13. Prejdite na stránku **Autentifikácia**.
14. V poli **Názov lokálneho hostiteľa** zadajte názov hostiteľa lokálneho servera kľúčov SystemB.
15. Kliknutím na **OK** uložíte popis novej virtuálnej linky a vrátite sa na stránku **Pripojenie**.
16. Prejdite na stránku **Nastavenia TCP/IP**.
17. V časti **Lokálna adresa IP** vyberte Pevná adresa IP lokálneho systému, 10.6.11.1.
18. V časti **Vzdialená adresa IP** vyberte **Adresová oblasť** ako metódu priradenia adresy. Zadajte začiatočnú adresu a potom zadajte počet adries, ktoré možno priradiť vzdialenému systému.
19. Vyberte **Povoliť vzdialenému systému prístup na iné siete (postupovanie IP)**.
20. Prejdite na stránku **Autentifikácia** a nastavte meno užívateľa a heslo pre tento profil PPP.
21. V časti Identifikácia lokálneho systému vyberte **Povoliť vzdialenému systému overovať totožnosť tohto systému**. Toto otvorí dialógové okno **Lokálna identifikácia systému**.
22. V časti **Autentifikačný protokol na použitie** vyberte **Vyžadovať zašifrované heslo (CHAP-MD5)**.
23. Zadajte meno užívateľa SystemB a heslo.
24. Kliknite na **OK** a uložíte profil PPP.

Aktivácia pravidiel pre pakety

Sprievodca VPN automatický vytvorí pravidlá pre pakety, ktoré sú nevyhnutné pre správne fungovanie tohto pripojenia. Ale než budete môcť spustiť pripojenie VPN, musíte ich aktivovať na oboch systémoch.

Pri aktivácii pravidiel pre pakety v Systéme A postupujte podľa týchto krokov:

1. V System i Navigator rozviňte **Systém A → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Aktivovať**. Toto otvorí dialógové okno **Aktivovať pravidlá pre pakety**.
3. Vyberte, či chcete aktivovať len vygenerované pravidlá VPN, len vybraný súbor alebo aj vygenerované pravidlá VPN aj vybraný súbor. Druhú možnosť môžete vybrať, ak napríklad máte rôznorodé pravidlá PERMIT a DENY, ktoré chcete vynútiť na rozhraní okrem vygenerovaných pravidiel VPN.
4. Vyberte rozhranie, na ktorom chcete aktivovať pravidlá. V tomto prípade vyberte **Všetky rozhrania**.
5. V dialógovom okne kliknite na **OK**, čím potvrdíte, že si želáte overiť a aktivovať pravidlá na zadaných rozhraniach. Keď kliknete na OK, systém skontroluje pravidlá pre syntaktické a sémantické chyby ohlási výsledky v okne správy v spodnej časti editora. Chybové správy, ktoré sú spojené s určitým súborom a číslom riadka, získate, keď kliknete pravým tlačidlom na chybu a vyberiete **Prejsť na riadok**, čím zvýrazníte chybu v súbore.
6. Zopakovaním týchto krokov aktivujte aj pravidlá pre pakety v Systéme B.

Scenár: VPN využívajúca firewally

V tomto scenári chce veľká poisťovacia spoločnosť vytvoriť VPN medzi bránou v Chicagu a hostiteľom v Minneaplise, pričom obe siete sa nachádzajú za firewallom.

Situácia

Predpokladajte, že ste poisťovacia spoločnosť pre vlastníka veľkého domu nachádzajúca sa v Minneapolise a práve ste otvorili novú pobočku v Chicagu. Pobočka v Chicagu vyžaduje prístup k databáze zákazníkov z centrály v Minneapolise. Chcete zaručiť bezpečnosť prenášaných informácií, pretože databáza obsahuje dôverné informácie o vašich zákazníkoch, napríklad mená, adresy a telefónne čísla. Rozhodli ste sa prepojiť obe pobočky cez internet prostredníctvom virtuálnej súkromnej siete (VPN). Obe pobočky sa nachádzajú za firewallmi a na utajenie svojich neregistrovaných súkromných IP adries pomocou sady registrovaných IP adries využívajú prekladanie sieťových adries (NAT). Je známe, že pripojenia VPN nie sú kompatibilné s NAT. Pripojenie VPN ruší pakety odosielané cez zariadenie NAT, pretože NAT mení adresu IP v pakete, čím ruší platnosť paketu. Stále však môžete použiť pripojenie VPN s NAT, ak implementujete zapuzdrenie UDP.

V tomto scenári je súkromná IP adresa zo siete v Chicagu vložená do novej hlavičky IP, a potom je pri prechode Firewallom C preložená (viď nasledujúci obrázok). Keď sa paket dostane na Firewall D, ten preloží cieľovú IP adresu na IP adresu Systému E a paket bude odoslaný ďalej Systému E. Nakoniec, keď sa paket dostane do Systému E, ten zruší hlavičku UDP, čím ostane len pôvodný paket IPSec, ktorý následne prejde všetkými overeniami platnosti a umožní bezpečné pripojenie VPN.

Ciele

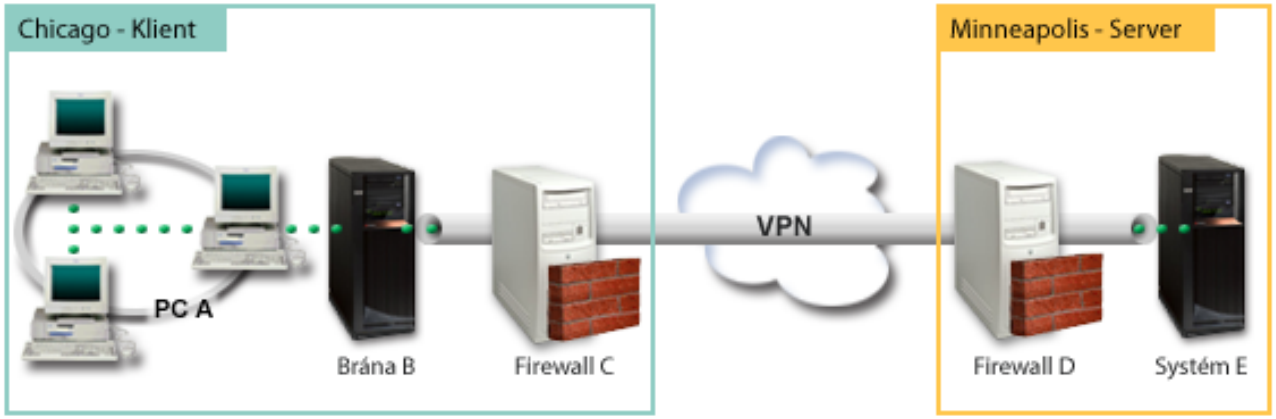
V tomto scenári chce veľká poisťovacia spoločnosť vytvoriť VPN medzi bránou v Chicagu (klient) a hostiteľom v Minneaplise (server), pričom obe siete sa nachádzajú za firewallom.

Ciele tohto návrhu sú nasledujúce:

- Brána pobočky v Chicagu vždy spúšťa pripojenie k hostiteľovi v Minneapolise.
- VPN musí ochraňovať celú dátovú prevádzku medzi bránou v Chicagu a hostiteľom v Minneapolise.
- Umožnite všetkým užívateľom brány v Chicagu pristupovať prostredníctvom pripojenia VPN k databáze System i umiestnenej v sieti Minneapolisu.

Detaily

Nasledujúci obrázok ilustruje charakteristiky siete pre tento návrh.



Sieť v Chicagu - Klient

- Brána B je spustená na i5/OS verzia 5 vydanie 4 (V5R4) alebo novšia.

- Brána B je k internetu pripojená s IP adresou 214.72.189.35 a je koncovým bodom tunelu VPN. Brána B vykonáva vyjednávania IKE a na odchádzajúce datagramy IP využíva zapuzdrenie UDP.
- Brána B a PC A sa nachádza v podsieti 10.8.11.0 s maskou 255.255.255.0.
- PC A je zdrojom a cieľom údajov, ktoré pretekajú pripojením VPN, preto je koncovým bodom údajov v tuneli VPN.
- Pripojenie k Systému E môže iniciovať len Brána B.
- Firewall C má pravidlo Masq NAT s verejnou IP adresou 129.42.105.17, za ktorou sú ukryté IP adresy v Bráne B.

Sieť v Minneapolise - Server

- Systém E je spustený na i5/OS verzia 5 vydanie 4 (V5R4) alebo novšia.
- Systém E má IP adresu 56.172.1.1.
- Systém E je v tomto scenári odpovedačom.
- Firewall D má IP adresu 146.210.18.51.
- Firewall D má pravidlo Static NAT, ktoré mapuje verejnú IP adresu (146.210.18.15) na súkromnú IP adresu Systému E (56.172.1.1). Preto z pohľadu klientov verejná IP adresa (146.210.18.51) Firewallu D predstavuje IP adresu Systému E.

Úlohy konfigurovania

Súvisiace koncepty

“Správa kľúčov” na strane 6
Dynamická VPN zabezpečuje dodatočnú bezpečnosť pre vašu komunikáciu pomocou protokolu Internet Key Exchange (IKE) pre správu kľúčov. IKE umožňuje VPN serverom na oboch koncoch pripojenia vyjednávať v určených intervaloch nové kľúče.

“IPSec s UDP kompatibilné s NAT” na strane 9
Zapuzdrenie UDP umožňuje prenosu IPSec prechádzať konvenčným zariadením NAT. Prezrite si túto tému, v ktorej nájdete viac informácií o tom, čo to je a prečo by ste to mali používať pre vaše pripojenia VPN.

Vyplnenie plánovacích pracovných listov

Nasledujúce plánovacie kontrolné zoznamy ilustrujú typ informácií, ktoré budete potrebovať pred samotnou konfiguráciou VPN. Skôr ako budete pokračovať v nastavovaní VPN, musia byť všetky odpovede v zozname nevyhnutných podmienok nastavené na YES.

Poznámka: Pre Bránu B a Systém E existujú osobitné pracovné listy.

Tabuľka 5. Systémové požiadavky

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je váš operačný systém i5/OS V5R4 alebo novší?	Áno
Máte nainštalovanú voľbu Správca digitálnych certifikátov?	Áno
Je nainštalované System i Access for Windows?	Áno
Je nainštalované System i Navigator?	Áno
Je nainštalovaný sieťový podkomponent System i Navigator?	Áno
Je nainštalované IBM TCP/IP Connectivity Utilities for i5/OS?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Máte vo vašom systéme nakonfigurované TCP/IP (vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény)?	Áno
Je medzi požadovanými koncovými bodmi vytvorená normálna komunikácia TCP/IP?	Áno
Použili ste najnovšie dočasné opravy programu (PTF)?	Áno
Ak VPN tunel traverzuje firewaly alebo smerovače používajúce filtrovanie IP paketov , podporujú filtrovacie pravidlá firewalu alebo smerovača protokoly AH a ESP?	Áno

Tabuľka 5. Systémové požiadavky (pokračovanie)

Kontrolný zoznam nevyhnutných požiadaviek	**Odpovede**
Sú firewally alebo smerovače nakonfigurované na povolenie premávky cez port 4500 pre dohodovania kľúčov? VPN partneri vykonávajú dohodovania IKE typicky cez port UDP 500, aj keď IKE zistí, že pakety NAT sú odosielané cez port 4500.	Áno
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	Áno

Tabuľka 6. Konfigurácia Brány B

Tieto informácie potrebujete pri konfigurácii VPN pre Bránu B.	**Odpovede**
Aký typ pripojenia vytvárate?	Brána k inému hostiteľovi
Ako pomenujete skupinu dynamických kľúčov?	CHIgw2MINhost
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov?	Vyvážený
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	Nie: topsecretstuff
Aký je identifikátor lokálneho servera kľúčov?	Adresa IP: 214.72.189.35
Aký je identifikátor lokálneho koncového bodu údajov?	Podsieť: 10.8.11.0 Maska: 255.255.255.0
Aký je identifikátor vzdialeného servera kľúčov?	Adresa IP: 146.210.18.51
Aký je identifikátor vzdialeného koncového bodu údajov?	Adresa IP: 146.210.18.51
Ktorým portom a protokolom chcete povoliť prenos cez pripojenie?	Všetkým
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich údajov?	Vyvážený
Na ktoré rozhrania sa pripojenie aplikuje?	TRLINE

Tabuľka 7. Konfigurácia Systému E

Tieto informácie potrebujete pri konfigurácii VPN pre Systém E.	**Odpovede**
Aký typ pripojenia vytvárate?	Hostiteľ k inej bráne
Ako pomenujete skupinu dynamických kľúčov?	CHIgw2MINhost
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov?	najvyššiu
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	Nie: topsecretstuff
Aký je identifikátor lokálneho servera kľúčov?	Adresa IP: 56.172.1.1
Aký je identifikátor vzdialeného servera kľúčov? **Poznámka:** Ak nie je známa IP adresa Firewallu C, môžete ako identifikátor vzdialeného servera kľúčov použiť *ANYIP.	Adresa IP: 129.42.105.17
Aký je identifikátor vzdialeného koncového bodu údajov?	Podsieť: 10.8.11.0 Maska: 255.255.255.0
Ktorým portom a protokolom chcete povoliť prenos cez pripojenie?	Všetkým
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich údajov?	najvyššiu
Na ktoré rozhrania sa pripojenie aplikuje?	TRLINE

Súvisiaci odkaz

Poradca pre plánovanie VPN

Konfigurácia VPN na Bráne B

Dokončením nasledujúcich krokov môžete nakonfigurovať pripojenie VPN v Bráne B.

Pri konfigurácii VPN v Bráne B použite nasledujúcim spôsobom informácie z vašich plánovacích pracovných listov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.

2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Pripojenie.
3. Zobrazte **uvítaciu** stránku, kde nájdete informácie o objektoch, ktoré sprievodca vytvorí.
4. Kliknite na **Ďalej** a prejdite na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte CHIgw2MINhost.
6. Voliteľné: Zadajte opis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdite na stránku **Scenár pripojení**.
8. Vyberte **Pripojiť vašu bránu k inému hostiteľovi**.
9. Kliknite na **Ďalej** a prejdite na stránku **Politika Internet Key Exchange**.
10. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**.

    Poznámka: Ak prijmete chybovú správu, v ktorej je uvedené ″Požiadavka o certifikát sa nedala spracovať″, môžete ju ignorovať, pretože nepoužívate certifikáty pre výmenu kľúčov.
11. Voliteľné: Ak máte certifikáty nainštalované, zobrazí sa stránka **Certifikát pre koncový bod lokálneho pripojenia**. Vyberte Nie, aby ste naznačili, že certifikáty chcete používať na autentifikáciu pripojenia.
12. Kliknite na **Ďalej** a prejdete na stránku **Lokálny server kľúčov**.
13. V poli **Typ identifikátora** vyberte **IP verzie 4**.
14. V poli **Adresa IP** vyberte 214.72.189.35.
15. Kliknite na **Ďalej** a prejdite na stránku **Vzdialený server kľúčov**.
16. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
17. V poli **Identifikátor** zadajte 146.210.18.51.

    Poznámka: Gateway B vytvorí pripojenie k statickému NAT a musíte zadať výmenu kľúčov hlavného režimu, aby ste mohli zadať samostatnú adresu IP pre vzdialený kľúč. Ak pripojenie vytvoríte pomocou Sprievodcu pripojením VPN, výmena kľúčov hlavného režimu je vybratá predvolene. Ak v tejto situácii použijete agresívny režim, zo vzdialeného kľúča musíte zadať vzdialený identifikátor iného typu ako IPV4.
18. V poli **Predzdieľaný kľúč** zadajte topsecretstuff.
19. Kliknite na **Ďalej** a prejdete na stránku **Lokálny koncový bod údajov**.
20. V poli **Typ identifikátora** vyberte **Podsieť 4 verzie IP** .
21. V poli **Identifikátor** zadajte 10.8.0.0.
22. V poli **Maska podsiete** zadajte 255.255.255.0.
23. Kliknite na **Ďalej** a prejdite na stránku **Služby údajov**.
24. Použite predvolené hodnoty a potom kliknite na **Ďalej**, aby ste prešli na stránku Politika údajov.
25. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**.
26. Kliknite na **Ďalej** a prejdite na stránku **Použiteľné rozhrania**.
27. Z tabuľky Linka vyberte **TRLINE**.
28. Kliknite na **Ďalej** a prejdete na stránku **Súhrn**.
29. Prezrite objekty, ktoré vytvorí sprievodca a presvedčte sa, či sú správne.
30. Kliknutím na **Dokončiť** dokončíte konfiguráciu.
31. Po zobrazení dialógového okna **Aktivovať filtre politík** vyberte **Áno**, aktivujte vygenerované filtre politík a vyberte **Povoliť každú inú premávku**.
32. Kliknutím na **OK** dokončíte konfiguráciu.

Konfigurácia VPN v Systéme E

Dokončením nasledujúcich krokov môžete nakonfigurovať pripojenie VPN v Systéme E.

Pri konfigurácii VPN v Systéme E použite nasledujúcim spôsobom informácie z vašich plánovacích pracovných listov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Pripojenie.
3. Zobrazte **uvítaciu** stránku, kde nájdete informácie o objektoch, ktoré sprievodca vytvorí.
4. Kliknite na **Ďalej** a prejdite na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte CHIgw2MINhost.
6. Voliteľné: Zadajte opis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdite na stránku **Scenár pripojení**.
8. Vyberte **Pripojiť vášho hostiteľa k inej bráne**.
9. Kliknite na **Ďalej** a prejdite na stránku **Politika Internet Key Exchange**.
10. Vyberte **Vytvoriť novú politiku** a potom vyberte **Vyvážená bezpečnosť a výkon**.

    Poznámka: Ak prijmete chybovú správu, v ktorej je uvedené ″Požiadavka o certifikát sa nedala spracovať″, môžete ju ignorovať, pretože nepoužívate certifikáty pre výmenu kľúčov.
11. Voliteľné: Ak máte certifikáty nainštalované, zobrazí sa stránka **Certifikát pre koncový bod lokálneho pripojenia**. Vyberte Nie, aby ste naznačili, že certifikáty chcete používať na autentifikáciu pripojenia.
12. Kliknite na **Ďalej** a prejdete na stránku **Lokálny server kľúčov**.
13. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
14. V poli **adresa IP** vyberte 56.172.1.1.
15. Kliknite na **Ďalej** a prejdite na stránku **Vzdialený server kľúčov**.
16. V poli **Typ identifikátora** vyberte **Adresa IP verzie 4**.
17. V poli **Identifikátor** zadajte 129.42.105.17.

    Poznámka: Ak nie je známa IP adresa Firewallu C, môžete ako identifikátor vzdialeného servera kľúčov použiť *ANYIP.
18. V poli **Predzdieľaný kľúč** zadajte topsecretstuff.
19. Kliknite na **Ďalej** a prejdete na stránku **Vzdialený koncový bod údajov**.
20. V poli **Typ identifikátora** vyberte **Podsieť 4 verzie IP** .
21. V poli **Identifikátor** zadajte 10.8.11.0.
22. V poli **Maska podsiete** zadajte 255.255.255.0.
23. Kliknite na **Ďalej** a prejdite na stránku **Služby údajov**.
24. Použite predvolené hodnoty a potom kliknite na **Ďalej**, aby ste prešli na stránku Politika údajov.
25. Vyberte **Vytvoriť novú politiku** a potom vyberte **Vyvážená bezpečnosť a výkon**.
26. Kliknite na **Ďalej** a prejdite na stránku **Použiteľné rozhrania**.
27. Z tabuľky Linka vyberte **TRLINE**.
28. Kliknite na **Ďalej** a prejdete na stránku **Súhrn**.
29. Prezrite objekty, ktoré vytvorí sprievodca a presvedčte sa, či sú správne.
30. Kliknutím na **Dokončiť** dokončíte konfiguráciu.
31. Po zobrazení dialógového okna **Aktivovať filtre politík** vyberte **Áno**, aktivujte vygenerované filtre politík a vyberte **Povoliť každú inú premávku**.
32. Kliknutím na **OK** dokončíte konfiguráciu.

Spustenie pripojenia

Ak ste už vaše pripojenie VPN v Systéme E nakonfigurovali, potrebujete toto pripojenie VPN spustiť.

Nasledujúcim postupom si môžete potvrdiť, či je aktívne pripojenie CHIgw2MINhost v Systéme E:

1. V System i Navigator **rozviňte Systém E → Network → Secure Connections → All Connections**.
2. Zobrazte **CHIgw2MINhost** a skontrolujte, že pole **Stav** má hodnotu *Nečinné* alebo *Na požiadanie*.

Pri spustení pripojenia CHIgw2MINhost z Brány B postupujte podľa týchto krokov:

1. V System i Navigator **rozviňte Bránu B → Network → IP Policies**.
2. Ak nie je server VPN spustený, kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Spustiť**.
3. Rozviňte **Budovanie VPN → Bezpečné pripojenia**.
4. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
5. Pravým tlačidlom myši kliknite na **CHIgw2MINhost** a vyberte **Spustiť**.
6. Z ponuky **Zobrazenie** vyberte **Obnoviť**. Ak je pripojenie úspešne spustené, hodnota poľa **Stav** sa zmení zo *Spúšťa sa* alebo *Na požiadanie* na *Povolené*. Spúšťanie pripojenia môže chvíľu trvať, preto pravidelne obnovujte okno, až kým sa jeho stav nezmení na *Povolený*.

Testovanie pripojenia

Po dokončení konfigurácie na Bráne B a v Systéme E a po úspešnom spustení serverov VPN otestujte pripojiteľnosť, aby ste sa overili, či môžu oba systémy navzájom komunikovať.

Pri testovaní vašich pripojení postupujte podľa týchto krokov:

1. Nájdite systém v sieti PC A a otvorte reláciu Telnet.
2. Zadajte verejnú IP adresu Systému E, teda 146.210.18.51.
3. Zadajte akékoľvek vyžadované prihlasovacie informácie. Ak dokážete zobraziť prihlasovaciu obrazovku, pripojenie je funkčné.

Scenár: pripojenie VPN k vzdialeným užívateľom

Aby mohol administrátor povoliť vzdialené pripojenia, potrebuje nakonfigurovať pripojenie virtuálnej súkromnej siete (VPN) k vzdialeným užívateľom.

V nasledujúcej úlohe je popísané ako administrátor nakonfiguruje pripojenie VPN k vzdialeným užívateľom.

Vypĺňanie plánovacích pracovných listov pripojenia VPN medzi pobočkou spoločnosti a vzdialenými obchodníkmi

Ako pomoc pri konfigurácii virtuálnej súkromnej siete (VPN) v systémoch a na vzdialených pracovných staniciach obchodnej pobočky využíva administrátor dynamické plánovacie pracovné listy, ktoré vytvára pomocou nástroja plánovací poradca VPN.

Plánovací poradca VPN je interaktívny nástroj, ktorý kladie konkrétne otázky a hodnotí vaše potreby týkajúce sa VPN. V závislosti na vašich odpovediach poradca vygeneruje plánovací pracovný list prispôsobený vášmu prostrediu, ktorý môžete použiť pri konfigurácii vášho pripojenia VPN. Tento pracovný list môžete neskôr použiť pri konfigurácii VPN vo vašom systéme. Každý z nasledujúcich pracovných listov generuje plánovací poradca VPN a všetky je možné použiť pri konfigurácii VPN pomocou sprievodcu Nové pripojenie VPN v System i Navigator.

Tabuľka 8. Plánovací pracovný list pripojenia VPN medzi obchodnou pobočkou a vzdialenými obchodníkmi

Otázky sprievodcu VPN	**Odporúčania poradcu VPN**
Ako by ste chceli nazvať túto skupinu pripojení?	SalestoRemote
Aký typ skupiny pripojenia by ste chceli vytvoriť?	Vyberte **Connect your host to another host**
Akú politiku IKE (Internet Key Exchange) chcete použiť na ochranu vašich kľúčov?	Vyberte **Create a new policy** , a potom vyberte **highest security, lowest performance**
Používate certifikáty?	Vyberte **No**

Tabuľka 8. Plánovací pracovný list pripojenia VPN medzi obchodnou pobočkou a vzdialenými obchodníkmi (pokračovanie)

Otázky sprievodcu VPN	Odporúčania poradcu VPN
Zadajte identifikátor, ktorý predstavuje lokálny server kľúčov tohto pripojenia.	Typ identifikátora: **IP version 4 address**, IP adresa:**192.168.1.2**. V prípade IPv6 adresy zadajte typ identifikátora: **IP version 6 address**, IP adresa:**2001:DB8::2** **Poznámka:** IP adresy, ktoré sú v tomto scenári použité, slúžia výhradne ako príklady. Neodrážajú schému IP adresovania, a preto by nemali byť použité v skutočných konfiguráciách. Pri dokončení týchto úloh by ste mali použiť vlastné IP adresy.
Aký je identifikátor servera kľúčov, ku ktorému sa chcete pripojiť?	Typ identifikátora: **Any IP address**, **Pre-shared key**: mycokey. **Poznámka:** Predzdieľaný kľúč je 32-znakový textový reťazec, ktorý VPN v i5/OS využíva tak pri autentifikácii pripojenia, ako aj pri vytváraní kľúčov, ktorými sú chránené vaše údaje. Vo všeobecnosti by ste s predzdieľaným kľúčom mali zaobchádzať rovnako, ako s vaším heslom.
Aké sú porty a protokoly údajov, ktoré bude toto pripojenie chrániť?	**Local Port**: 1701, **Remote Port**: Ktorýkoľvek port, **Protocol**: UDP
Ktorú politiku údajov chcete využívať pri ochrane údajov?	Vyberte **Create a new policy**, a potom vyberte **highest security, lowest performance**
Označte rozhrania na lokálnom systéme, na ktorých bude toto pripojenie použité.	ETHLINE (Obchodná pobočka)

Konfigurácia profilu terminátora L2TP Systému A

Ak chcete nakonfigurovať vzdialené pripojenia k vzdialeným pracovným staniciam, potrebujete nastaviť Systém A tak, aby akceptoval pripojenia prichádzajúce od týchto klientov.

Pri konfigurácii profilu terminátora L2TP (Layer Two Tunneling Protocol) pre Systém A vykonajte nasledujúce kroky:

1. V System i Navigator rozviňte ***Systém A*** → **Network** → **Remote Access Services**.
2. Ak chcete nastaviť Systém A ako server, ktorý umožňuje pripojenia prichádzajúce od vzdialených užívateľov, kliknite pravým tlačidlom myši na **Receiver Connection Profiles** a vyberte **New Profile**.
3. Na stránke Setup vyberte nasledujúce voľby:
   - **Protocol type:** PPP
   - **Connection type:** L2TP (virtuálna linka)

     Poznámka: V poli **Operating mode** by malo byť automaticky zobrazené **Terminator (network server)**.
   - **Line service type:** Jediná linka
4. Kliknite na **OK**. Tým zobrazíte stránku New Point-to-Point Profile Properties.
5. Na záložke **Všeobecné** vyplňte tieto polia:

- **Name**: MYCOL2TP
- Ak chcete, aby bol tento profil automaticky spúšťaný s TCP, vyberte **Start profile with TCP**.

6. Ako **Local tunnel endpoint IP address** v záložke **Connection** vyberte **192.168.1.2** (v prípade IPv6 vyberte **2001:DB8::2**).

   Dôležité: IP adresy, ktoré sú v tomto scenári použité, slúžia výhradne ako príklady. Neodrážajú schému IP adresovania, a preto by nemali byť použité v skutočných konfiguráciách. Pri dokončení týchto úloh použite vlastné IP adresy.
7. Ako **Virtual line name** vyberte **MYCOL2TP**. Tým zobrazíte stránku New L2TP Properties.
8. Ako názov hostiteľa na stránke Authentication zadajte systema. Kliknite na **OK**. Tým sa vrátite na stránku Connection.
9. Na stránke Connection vyberte nasledujúce voľby a ako **Maximum number of connections** zadajte 25.
   a. Kliknite na záložku **Authentication** a vyberte **Require this system to verify the identity of the remote system**.
   b. Vyberte **Authenticate locally with validation list**.
   c. V poli **Validation list name** zadajte QL2TP a kliknite na **New**.
10. Na stránke Validation list vyberte **Add**.
11. Pridajte meno užívateľa a heslo každého z vašich vzdialených zamestnancov. Kliknite na **OK**.
12. Na stránke Password confirmation znova zadajte heslo pre každého z vašich vzdialených zamestnancov. Kliknite na **OK**.
13. Ako **Local IP address** na stránke TCP/IP Setting vyberte 10.1.1.1 (v prípade IPv6 vyberte 2001:DA8::1).
14. V poli **IP address assignment method** vyberte **Address pool**.
15. V poli **Starting IP address** zadajte 10.1.1.100 a ako **Number of addresses** zadajte 49. V prípade IPv6 adresy v poli **Starting IP address** zadajte 2001:DA8::1:1 a ako **Number of addresses** zadajte 65535.
16. Vyberte **Povoliť vzdialenému systému prístup na iné siete (postupovanie IP)**. Kliknite na **OK**.

Spustenie profilu pripojenia prijímača

Po nakonfigurovaní profilu pripojenia prijímača L2TP (Layer Two Tunneling Protocol) pre Systém A potrebuje administrátor toto pripojenie spustiť, aby mohlo počúvať prichádzajúce požiadavky vzdialených klientov.

Poznámka: Možno bude zobrazené chybové hlásenie, v ktorom bude napísané, že podsystém QUSRWRK nie je spustený. Táto správa je zobrazená pri pokuse o spustenie profilu pripojenia prijímača. Ak chcete spustiť podsystém QUSRWRK, vykonajte tieto kroky:

1. V znakovom rozhraní zadajte strsbs.
2. V poli **Subsystem description** obrazovky Start Subsystem zadajte QUSRWRK.

Ak chcete spustiť profil pripojenia prijímača pre vzdialených klientov, vykonajte tieto úlohy:

1. V System i Navigator vyberte v ponuke **View** položku **Refresh**. Tým obnovíte vašu inštanciu System i Navigator.
2. V System i Navigator rozviňte ***System A*** **→ Network → Remote Access Services**.
3. Kliknite dva razy na **Receiver Connection Profiles**, pravým tlačidlom myši kliknite na **MYCOL2TP** a vyberte **Start**.
4. V poli **Status** bude zobrazené **Waiting for connection requests**.

Konfigurácia pripojenia VPN v Systéme A pre vzdialených klientov

Po nakonfigurovaní a spustení profilu pripojenia prijímača L2TP (Layer Two Tunneling Protocol) pre Systém A potrebuje administrátor nakonfigurovať virtuálnu súkromnú sieť (VPN), ktorá bude chrániť toto pripojenie medzi vzdialenými klientmi a sieťou obchodnej pobočky.

VPN pre vzdialených klientov nakonfigurujete vykonaním týchto krokov:

Dôležité: IP adresy, ktoré sú v tomto scenári použité, slúžia výhradne ako príklady. Neodrážajú schému IP adresovania, a preto by nemali byť použité v skutočných konfiguráciách. Pri dokončení týchto úloh použite vlastné IP adresy.

1. V System i Navigator rozviňte ***Systém A*** → **Network** → **IP Policies**.
2. Kliknite pravým tlačidlom myši na položku **Virtual Private Networking** a výberom **New Connection** spustite sprievodcu Nové pripojenie VPN. Na jeho uvítacej stránke nájdete informácie o tom, aké objekty tento sprievodca vytvára.
3. Kliknutím na **Next** prejdite na stránku Connection Name.
4. V poli **Name** zadajte SalestoRemote.
5. Voliteľný: Zadajte popis tejto skupiny pripojení. Kliknite na tlačidlo **Ďalej**.
6. Na stránke Connection Scenario vyberte **Connect your host to another host**. Kliknite na **Next**.
7. Na stránke Internet Key Exchange Policy vyberte **Create a new policy**, a potom vyberte **Highest security, lowest performance**. Kliknite na tlačidlo **Ďalej**.
8. Na stránke Certificate for Local Connection Endpoint vyberte **No**. Kliknite na tlačidlo **Ďalej**.
9. Ako typ identifikátora na stránke Local Key Server vyberte **Version 4 IP address**. Priradená IP adresa by mala byť 192.168.1.2. Kliknite na tlačidlo **Ďalej**. V prípade IPv6 adresy vyberte na stránke Local Key Server typ identifikátora **Version 6 IP address**. Priradená IP adresa by mala byť 2001:DB8::2. Kliknite na **Next**.
10. V poli **Identifier type** na stránke Remote Key Server vyberte **Any IP address**. V poli **Pre-shared key** zadajte mycokey. Kliknite na tlačidlo **Ďalej**.
11. Ako lokálny port na stránke Data Services zadajte 1701. Potom ako vzdialený port vyberte 1701 a vyberte protokol **UDP**. Kliknite na tlačidlo **Ďalej**.
12. Na stránke Data Policy vyberte **Create a new policy**, a potom vyberte **Highest security, lowest performance**. Kliknite na tlačidlo **Ďalej**.
13. Na stránke Applicable Interfaces vyberte **ETHLINE**. Kliknite na tlačidlo **Ďalej**.
14. Na stránke Summary skontroluje objekty, ktoré sprievodca vytvorí a uistite sa, či sú správne.
15. Kliknutím na **Dokončiť** dokončíte konfiguráciu. Pri otvorení okna Activate Policy Filters vyberte **No, packet rules will be activated at a later time**. Kliknite na **OK**.

Aktualizácia politík VPN pre vzdialené pripojenia z klientov Windows XP a Windows 2000

Keďže sprievodca vytvára štandardné pripojenie, ktoré je možné využiť vo väčšine konfigurácií virtuálnych súkromných sietí (VPN), ak chcete zabezpečiť dotykovú prevádzkyschopnosť s klientmi Windows XP a Windows 2000, budete musieť tieto sprievodcom vygenerované politiky aktualizovať.

Pri aktualizácií týchto politík VPN vykonajte nasledujúce úlohy:

1. V System i Navigator rozviňte ***Systém A*** → **Network** → **IP Policies** → **Virtual Private Networking** → **IP Security Policies**.
2. Kliknite dva razy na **Internet Key Exchange Policies**, pravým tlačidlom myši kliknite na **Any IP address** a vyberte **Properties**.
3. Na stránke Transform kliknite na **Add**.
4. Na stránke Add Internet Key Exchange Transform vyberte nasledujúce voľby:
   - **Authentication method:** Predzdieľaný kľúč
   - **Hash algorithm:** MD5
   - **Encryption algorithm:** DES-CBC
   - **Diffie-Hellman group:** Skupina 1
5. Kliknite na **OK**.
6. V System i Navigator rozviňte ***Systém A*** → **Network** → **IP Policies** → **Virtual Private Networking** → **IP Security Policies**.
7. Kliknite dva razy na **Data Policies**, kliknite pravým tlačidlom myši na **SalestoRemote** a vyberte **Properties**.

8. Na stránke General zrušte označenie **Use Diffie-Hellman perfect forward secrecy**.
9. Vyberte **ESP Proposal** a kliknite na **Edit**.
10. Voľby na stránke Data Policy Proposal upravte nasledujúcim spôsobom:
    - **Encapsulation mode:** Prenos
    - **Key expiration:** 15 minút
    - **Expire at size limit:** 100000
11. Na stránke Transform kliknite na **Add**.
12. Na stránke Add Data Policy Transform vyberte nasledujúce voľby:
    - **Protocol:** Encapsulating security payload (ESP)
    - **Authentication algorithm:** MD5
    - **Encryption algorithm:** DES-CBC
13. Dva razy kliknite na **OK**.

Aktivácia pravidiel filtrovania

Sprievodca automaticky vytvorí pravidlá pre pakety, ktoré toto pripojenie vyžaduje, aby mohol správne pracovať. Predtým, než spustíte virtuálnu súkromnú sieť (VPN), ich však musíte aktivovať na oboch systémoch.

Pri aktivácii pravidiel filtrovania v Systéme A postupujte podľa týchto krokov:

Dôležité: IP adresy, ktoré sú v tomto scenári použité, slúžia výhradne ako príklady. Neodrážajú schému IP adresovania, a preto by nemali byť použité v skutočných konfiguráciách. Pri dokončení týchto úloh by ste mali použiť vlastné IP adresy.

1. V System i Navigator rozviňte ***Systém A*** → **Network** → **IP Policies**.
2. kliknite pravým tlačidlo myši na položku **Packet Rules** a vyberte **Activate Rules**.
3. Na stránke Activate Packet Rules vyberte **activate only the VPN generated rules** a ako rozhranie, v ktorom by ste tieto pravidlá filtrovania chceli aktivovať, vyberte **ETHLINE**. Kliknite na **OK**.

Aby mohli vzdialení užívatelia nastaviť svoju stranu pripojenia, musí im administrátor poskytnúť nasledujúce informácie predtým, než budú konfigurovať svoje pracovné stanice Windows XP. Každému z vašich vzdialených užívateľov poskytnite nasledujúce informácie:

- názov predzdieľaného kľúča: mycokey,
- IP adresu Systému A: 192.168.1.2 (2001:DB8::2 in IPv6),
- meno užívateľa a heslo pre toto pripojenie.

Poznámka: Tieto položky boli vytvorené počas konfigurácie profilu terminátora L2TP (Layer Two Tunneling Protocol), keď administrátor pridal meno užívateľa a heslo do zoznamu kontroly platnosti.

Konfigurácia VPN na klientovi Windows XP

Pomocou tejto procedúry môžete nakonfigurovať VPN na klientovi Windows XP.

Pri nastavení vzdialených klientov Windows XP musia vzdialení užívatelia v MyCo, Inc vykonať nasledujúce kroky:

1. V ponuke **Start** vo Windows XP rozviňte **All Programs** → **Accessories** → **Communications** → **New Connection Wizard**.
2. Na uvítacej stránke si prečítajte súhrn informácií. Kliknite na tlačidlo **Ďalej**.
3. Na stránke Network Connection Type vyberte **Connect to the network at my workplace**. Kliknite na tlačidlo **Ďalej**.
4. Na stránke Network Connection vyberte **Virtual Private Network connection**. Kliknite na tlačidlo **Ďalej**.
5. V poli **Company Name** na stránke Connection Name zadajte Connection to Branch office. Kliknite na tlačidlo **Ďalej**.
6. Na stránke Public Network vyberte **Do not dial the initial connection**. Kliknite na tlačidlo **Ďalej**.

7. V poli **Host name or IP address** na stránke VPN Server Selection zadajte 192.168.1.2 (v prípade IPv6 zadajte 2001:DB8::2). Kliknite na tlačidlo **Ďalej**.
8. Na stránke Connection Availability vyberte **My Use Only**. Kliknite na tlačidlo **Ďalej**.
9. Na stránke Summary kliknite na **Add a shortcut to this connection to my desktop**. Kliknite na **Dokončiť**.
10. Kliknite na ikonu **Connect Connection to MyCo**, ktorá bola vytvorená na vašej pracovnej ploche.
11. Na stránke Connect Connection to MyCo page zadajte meno užívateľa a heslo, ktoré vám poskytol administrátor.
12. Vyberte **Save this user name and password for the following users** a **Me only**. Kliknite na **Vlastnosti**.
13. Na stránke **Security** sa uistite, či máte označené nasledujúce **Security options**:
    - **Typical**
    - **Require secured password**
    - **Require data encryption**

    Kliknite na **IPSec Settings**.
14. Na stránke IPSec Settings vyberte **Use pre-shared key for authentication** a v poli **Pre-shared key** zadajte mycokey. Kliknite na **OK**.
15. Ako **Type of VPN** na stránke Networking vyberte **L2TP IPSec VPN**. Kliknite na **OK**.
16. Prihláste sa pomocou mena užívateľa a hesla a kliknite na **Connect**.

Ak budete chcieť spustiť pripojenie k virtuálnej súkromnej sieti (VPN) na strane klienta, kliknite na ikonu, ktorá bola po dokončení sprievodcu pripojením pridaná na vašu pracovnú plochu.

Testovanie pripojenia VPN medzi koncovými bodmi

Po dokončení konfigurácie pripojenia medzi Systémom A a vzdialenými užívateľmi a po úspešnom spustení pripojenia by ste si mali otestovať ich pripojiteľnosť, aby ste si overili, či môžu vzdialení hostitelia navzájom komunikovať.

Pri testovaní pripojiteľnosti postupujte podľa týchto krokov:

1. V System i Navigator rozviňte ***Systém A*** → **Network**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia TCP/IP**, vyberte **Nástroje** a potom **Ping**.
3. V poli **Ping** v dialógovom okne **Ping from** zadajte 10.1.1.101 (v prípade IPv6 zadajte 2001:DA8::1:101).

   Poznámka: 10.1.1.101 predstavuje IP adresu dynamicky priradenú (vzdialeným obchodným klientom) z oblasti adries zadanej v profile terminátora L2TP (Layer Two Tunneling Protocol) v Systéme A.
4. Kliknutím na **Ping Now** overte pripojiteľnosť zo Systému A k vzdialeným pracovným staniciam. Kliknite na **OK**.

Pri testovaní pripojenia zo vzdialeného klienta na pracovnej stanici, na ktorej je spustený Windows, vykoná vzdialený zamestnanec tieto kroky:

1. V príkazovom riadku zadajte ping 10.1.1.2 (v prípade IPv6 zadajte ping 2001:DA8::2). Ide o IP adresu jednej z pracovných staníc siete v kancelárii podniku.
2. Opakovaním týchto krokov otestujte pripojiteľnosť z kancelárie podniku na pobočku spoločnosti.

Scenár: Použitie prekladania sieťových adries v pripojení VPN

V tomto scenári chce vaša spoločnosť vymeniť citlivé údaje s jedným zo svojich obchodných partnerov pomocou VPN. Aby spoločnosť ešte lepšie ochránila súkromie vlastnej štruktúry siete, použije VPN NAT na ukrytie súkromnej adresy IP systému, ktorý sa používa na hosťovanie aplikácií, ku ktorým má váš obchodný partner prístup.

Situácia

Predpokladajme, že ste sieťový administrátor v malej výrobnej spoločnosti v Minneapolise. Jeden z vašich obchodných partnerov, dodávateľ súčiastok v Chicagu, chce začať spracovávať väčšiu časť svojej agendy cez internet. Je rozhodujúce, aby vaša spoločnosť mala určité súčiastky a množstvá k dispozícii presne v určenom čase, keď ich

potrebuje, takže dodávateľ musí byť neustále informovaný o stave inventára a výrobných plánoch vašej spoločnosti. V súčasnosti túto interakciu zvládnete manuálne, ale zistíte, že je časovo náročná, nákladná a rovnako aj časovo nepresná, takže ste viac ako ochotní preskúmať svoje možnosti.

Keď vezmete do úvahy dôvernosť a časovo náročnú povahu informácií, ktoré si vymieňate, rozhodnete sa vytvoriť VPN medzi sieťou vášho dodávateľa a sieťou vašej spoločnosti. Aby ste ešte lepšie ochránili súkromie štruktúry siete vašej spoločnosti, rozhodnete sa skryť súkromnú adresu IP systému, ktorý sa používa na hosťovanie aplikácií, ku ktorým má váš dodávateľ prístup.

Virtuálne súkromné siete môžete použiť nielen na vytvorenie definícií pripojení v bráne VPN v sieti vašej spoločnosti, ale aj na preklad sieťových adries, ktorý potrebujete na ukrytie vašich lokálnych súkromných adries. Na rozdiel od zvyčajného prekladu sieťových adries (NAT), ktorý mení adresy IP v bezpečnostných asociáciách (SA), ktoré VPN vyžaduje pre svoju činnosť, VPN NAT vykonáva preklad adries pred kontrolou platnosti SA pomocou priraďovania adresy k pripojeniu, keď sa pripojenie spustí.

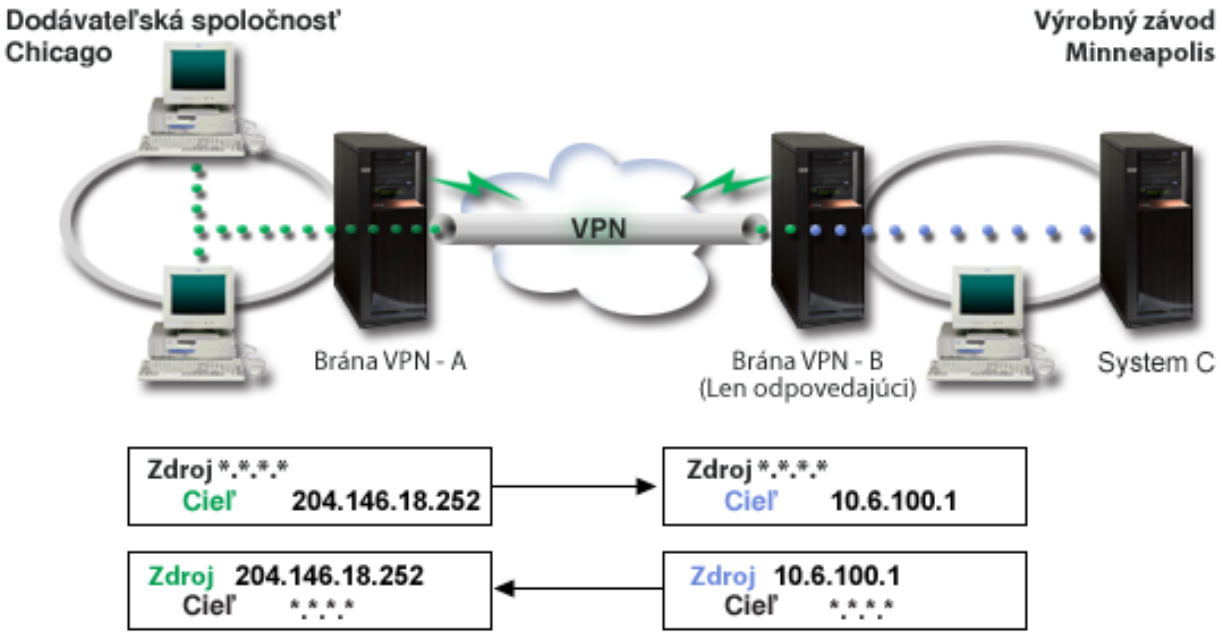
Ciele

Ciele tohto scenára sú:

- umožniť všetkým klientom v sieti dodávateľa prístup k samostatnému hostiteľskému systému v sieti výrobcu cez pripojenie VPN typu brána k bráne.
- skryť súkromnú adresu IP hostiteľského systému v sieti výrobcu jej preložením na verejnú adresu IP pomocou prekladu sieťových adries pre VPN (VPN NAT).

Detaily

Nasledujúci graf znázorňuje charakteristiky siete dodávateľa a siete výrobcu:



- Brána-A VPN sa nakonfiguruje tak, aby vždy zahajovala pripojenia na bránu-B VPN.
- Brána A pripojenia VPN určuje koncový bod pripojenia ako 204.146.18.252 (verejná adresa priradená Systému C).
- Systém C má súkromnú IP adresu v sieti výrobcu 10.6.100.1.
- Verejná adresa 204.146.18.252 bola v lokálnej servisnej oblasti na bráne B pripojenia VPN zadefinovaná ako súkromná adresa Systému C 10.6.100.1.

- Brána B pripojenia VPN preloží prichádzajúcim datagramom verejnú adresu Systému C do jeho súkromnej adresy 10.6.100.1. Brána B pripojenia VPN preloží vracajúce sa odchádzajúce datagramy z adresy 10.6.100.1 naspäť na verejnú adresu Systému C, teda 204.146.18.252. Z hľadiska klientov v dodávateľskej sieti má Systém C IP adresu 204.146.18.252. Klienti nikdy nezistia, že došlo k prekladu adries.

Úlohy konfigurovania

Ak chcete nakonfigurovať pripojenie opísané v tomto scenári, vykonajte každú z nasledujúcich úloh:

1. Nakonfigurovať základnú VPN typu brána-brána medzi **Bránou-A VPN** a **Bránou-B** VPN.
2. Zadefinovať lokálnu servisnú oblasť v **bráne B pripojenia VPN** a ukryť tak súkromnú adresu **Systému C** za verejný identifikátor 204.146.18.252.
3. Nakonfigurovať **Bránu-B VPN** na preklad lokálnych adries pomocou adries lokálnej servisnej oblasti.

Súvisiace koncepty

"Preklad sieťových adries pre VPN" na strane 8
VPN poskytuje prostriedky na preklad sieťových adries nazývaný VPN NAT. VPN NAT sa líši od zvyčajného NAT v tom, že prekladá adresy pred použitím protokolov IKE a IPSec. Obráťte sa na túto tému, v ktorej sa dozviete viac.

Plánovanie VPN

Prvým krokom správneho používania VPN je plánovanie. Táto téma vám poskytne informácie o migrácii z predchádzajúcich vydaní, požiadavkách na inštaláciu a odkazy na plánovacieho poradcu, ktorý vygeneruje plánovaciu tabuľku prispôsobenú vašim špecifikáciám.

Plánovanie je podstatná časť vášho celkového riešenia VPN. Je veľa zložitých rozhodnutí, ktoré musíte vykonať, aby ste zabezpečili, aby vaše pripojenie pracovalo správne. Použite tieto prostriedky na zhromaždenie všetkých informácií, ktoré budete potrebovať na to, aby bola vaša VPN úspešná:

- Požiadavky na nastavenie VPN
- Zistiť, aký typ VPN vytvoriť
- Použiť poradcu pre plánovanie VPN

  Poradca pre plánovanie vám bude klásť otázky o vašej sieti a na základe vašich odpovedí vám bude dávať návrhy na vytváranie vašej VPN.

  Poznámka: Poradcu pre plánovanie VPN použite len pre pripojenia, ktoré podporujú protokol IKE (Internet Key Exchange). Pre manuálne pripojenia pre vaše manuálne typy pripojenia použite plánovací pracovný hárok.
- Vyplniť plánovacie pracovné hárky VPN

Po naplánovaní vašej siete VPN môžete pristúpiť k jej konfigurácii.

Súvisiace úlohy

Použitie poradcu pre plánovanie VPN

"Konfigurácia VPN" na strane 45
Rozhranie VPN vám ponúka niekoľko rôznych spôsobov na konfiguráciu vašich pripojení VPN. Môžete nakonfigurovať manuálne alebo dynamické pripojenie.

Požiadavky na nastavenie VPN

Aby pripojenie VPN fungovalo správne tak vo vašom systéme ako aj so sieťovými klientmi, musíte splniť minimálne tieto požiadavky.

V nasledujúcom zozname sú vymenované minimálne požiadavky nastavenia pripojenia VPN:

Systémové požiadavky

- i5/OS verzia 5 vydanie 3 alebo novšia
- Správca digitálnych certifikátov
- System i Access for Windows
- System i Navigator
  - Sieťový komponent System i Navigator
- Nastaviť systémovú hodnotu bezpečnostných údajov servera (QRETSVRSEC *SEC) na 1
- TCP/IP musí byť nakonfigurovaný, vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény

Požiadavky na klienta

- Pracovná stanica s 32-bitovým operačným systémom Windows správne pripojená k vášmu systému a nakonfigurovaná pre TCP/IP
- Ústredná jednotka 233 Mhz
- Klienti pre Windows 95 s 32 MB RAM
- 64 MB RAM pre klientov Windows NT 4.0 a Windows 2000
- System i Access for Windows a System i Navigator nainštalované v PC klienta
- Softvér podporujúci protokol Bezpečnosť IP (IPSec)
- Softvér podporujúci L2TP, ak vzdialení užívatelia budú na vytvorenie pripojenia na váš systém používať L2TP

Súvisiace úlohy

"Začíname s odstraňovaním problémov s VPN" na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Rozhodnutia o type vytváranej VPN

Zisťovanie toho, ako budete používať svoju VPN, je jedným z prvých krokov pri úspešnom plánovaní. Za týmto účelom musíte pochopiť rolu, ktorú pri pripojení hrajú lokálny server kľúčov aj vzdialený server kľúčov.

Napríklad, sú koncové body *pripojenia* iné , než koncové body *údajov*? Sú rovnaké alebo sú kombináciou oboch? Koncové body pripojenia autentifikujú a šifrujú (alebo dešifrujú) prenos údajov pre pripojenie a voliteľne zabezpečujú správu kľúčov s protokolom Internet Key Exchange (IKE). Koncové body údajov ale definujú spojenie medzi dvoma systémami pre IP prenos, ktorý prebieha cez VPN; napríklad všetky TCP/IP prenosy medzi 123.4.5.6 a 123.7.8.9. Väčšinou, keď sú koncové body pripojenia a údajov rozdielne, server VPN je brána. Keď sú rovnaké, server VPN je hostiteľ.

Nasledujú rôzne typy implementácií VPN, ktoré veľmi dobre vyhovujú väčšine potrieb:

Brána-brána
Koncové body pripojenia oboch systémov sa líšia od koncových bodov údajov. Protokol Bezpečnosť IP (IPSec) ochraňuje prenos počas cesty medzi bránami. Ale IPSec neochraňuje prenos údajov ani na jednej strane brán v interných sieťach. Toto je spoločné nastavenie pre pripojenia medzi pobočkami, lebo prenos ktorý je smerovaný mimo brány pobočky do interných sietí, sa často považuje za dôveryhodný.

Brána-hostiteľ
IPSec ochraňuje prenos údajov počas cesty medzi vašou bránou a hostiteľom vo vzdialenej sieti. VPN neochraňuje prenos údajov v lokálnej sieti, lebo ho považujete za dôveryhodný.

Hostiteľ-brána
VPN ochraňuje prenos údajov počas cesty medzi hostiteľom v lokálnej sieti a vzdialenou bránou. VPN neochraňuje prenos údajov vo vzdialenej sieti.

Hostiteľ-hostiteľ
Koncové body pripojenia sú rovnaké ako koncové body údajov na lokálnom aj vzdialenom systéme. VPN ochraňuje prenos údajov počas cesty medzi hostiteľom v lokálnej sieti a hostiteľom vo vzdialenej sieti. Tento typ VPN zabezpečuje ochranu medzi koncami IPSec.

Vyplnenie plánovacích pracovných listov VPN

Pomocou plánovacích pracovných listov VPN môžete zozbierať podrobné informácie o plánovaní využitia vašej VPN. Aby ste mohli adekvátne naplánovať vašu stratégiu VPN, musíte vyplniť tieto pracovné listy. Tieto informácie môžete použiť aj na konfiguráciu vašej VPN.

Ak chcete, môžete tieto plánovacie pracovné listy vytlačiť a ich vyplnením zosumarizovať podrobné informácie týkajúce sa využitia vašej VPN.

Vyberte si pracovný list typu pripojenia, ktoré chcete vytvoriť.

- Plánovací pracovný list dynamického pripojenia
- Plánovací pracovný list manuálneho pripojenia
- Poradca pre plánovanie VPN

  Ak vám to viac vyhovuje, použite poradcu interaktívneho plánovania a konfigurácie. Poradca pre plánovanie vám bude klásť otázky o vašej sieti a na základe vašich odpovedí vám bude dávať návrhy na vytváranie vašej VPN.

  Poznámka: Poradcu pre plánovanie VPN použite len pre vaše dynamické pripojenia. Pre typy manuálnych pripojení použite plánovací pracovný list pre manuálne pripojenia.

Ak budete vytvárať niekoľko pripojení s podobnými vlastnosťami, budete možno chcieť nastaviť štandardné nastavenia VPN. Predvolené hodnoty, ktoré konfigurujete, pochádzajú z hárkov vlastností VPN. To znamená, že nemusíte konfigurovať rovnaké vlastnosti viackrát. Ak chcete nastaviť predvolené hodnoty VPN, z hlavnej ponuky VPN vyberte **Úpravy** a vyberte **Predvolené hodnoty**.

Súvisiace informácie

Poradca pre plánovanie VPN

Plánovací pracovný list dynamického pripojenia

Pred konfiguráciou dynamického pripojenia vyplňte tento pracovný list.

Predtým než budete vytvárať vaše dynamické pripojenia VPN, vyplňte tento pracovný list. Tento pracovný list predpokladá, že použijete sprievodcu Nové pripojenie. Sprievodca umožňuje nastaviť VPN na základe vašich základných bezpečnostných požiadaviek. Vlastnosti, ktoré tento sprievodca pre pripojenie nakonfiguruje, budete možno musieť v niektorých prípadoch spresniť. Môžete sa napríklad rozhodnúť, že vyžadujete žurnálovanie, alebo že chcete, aby bol pri každom spustení TCP/IP spustený server VPN. V takomto prípade kliknite pravým tlačidlom na skupinu dynamických kľúčov alebo pripojenie, ktoré vytvoril sprievodca a vyberte **Vlastnosti**.

Skôr ako budete v nastavovaní VPN pokračovať, odpovedzte na každú otázku.

Tabuľka 9. Systémové požiadavky

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je váš operačný systéme i5/OS V5R3 alebo novší?	Áno
Máte nainštalovanú voľbu Správca digitálnych certifikátov?	Áno
Je nainštalované System i Access for Windows?	Áno
Je nainštalované System i Navigator?	Áno
Je nainštalovaný sieťový podkomponent System i Navigator?	Áno
Je nainštalované IBM TCP/IP Connectivity Utilities for i5/OS?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Máte vo vašom systéme nakonfigurované TCP/IP (vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény)?	Áno
Je medzi požadovanými koncovými bodmi vytvorená normálna komunikácia TCP/IP?	Áno
Použili ste najnovšie dočasné opravy programu (PTF)?	Áno

Tabuľka 9. Systémové požiadavky (pokračovanie)

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Ak VPN tunel traverzuje firewaly alebo smerovače používajúce filtrovanie IP paketov , podporujú filtrovacie pravidlá firewalu alebo smerovača protokoly AH a ESP?	Áno
Sú firewally alebo smerovače nakonfigurované tak, aby povoľovali protokoly IKE (UDP port 500), AH a ESP?	Áno
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	Áno

Tabuľka 10. Konfigurácia VPN

Tieto informácie budete potrebovať na konfiguráciu dynamického pripojenia VPN	Odpovede
Aký typ pripojenia vytvárate? • Brána-brána • Hostiteľ-brána • Brána-hostiteľ • Hostiteľ-hostiteľ	
Ako pomenujete skupinu dynamických kľúčov?	
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov? • Najvyššia bezpečnosť, najnižší výkon • Vyváženie bezpečnosti a výkonnosti • Najnižšia bezpečnosť a najvyšší výkon	
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	
Aký je identifikátor lokálneho servera kľúčov?	
Aký je identifikátor lokálneho servera kľúčov?	
Aký je identifikátor vzdialeného servera kľúčov?	
Aký je identifikátor vzdialeného koncového bodu údajov?	
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich údajov? • Najvyššia bezpečnosť, najnižší výkon • Vyváženie bezpečnosti a výkonnosti • Najnižšia bezpečnosť a najvyšší výkon	

Plánovací pracovný list manuálneho pripojenia

Pred konfiguráciou manuálneho pripojenia vyplňte tento pracovný list.

Vyplnenie tohto pracovného listu vám pomôže pri vytváraní vášho pripojenia virtuálnej súkromnej siete (VPN), ktorá pri riadení kľúčov nevyužíva IKE. Skôr ako budete v nastavovaní VPN pokračovať, odpovedzte na každú z týchto otázok:

Tabuľka 11. Systémové požiadavky

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je v systém spustený i5/OS V5R3 alebo novší?	
Je nainštalovaný Správca digitálnych certifikátov?	
Je nainštalované System i Access for Windows?	
Je nainštalované System i Navigator?	
Je nainštalovaný sieťový podkomponent System i Navigator?	
Je nainštalované IBM TCP/IP Connectivity Utilities for i5/OS?	

Tabuľka 11. Systémové požiadavky (pokračovanie)

Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	
Máte vo vašom systéme nakonfigurované TCP/IP (vrátane rozhraní IP, trás, názvu lokálneho hostiteľa a názvu lokálnej domény)?	
Je medzi požadovanými koncovými bodmi vytvorená normálna komunikácia TCP/IP?	
Použili ste najnovšie dočasné opravy programu (PTF)?	
Ak VPN tunel traverzuje firewaly alebo smerovače používajúce filtrovanie IP paketov , podporujú filtrovacie pravidlá firewalu alebo smerovača protokoly AH a ESP?	
Sú firewally alebo smerovače nakonfigurované tak, aby povoľovali protokoly AH a ESP?	
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	

Tabuľka 12. Konfigurácia VPN

Tieto informácie budete potrebovať na konfiguráciu manuálneho VPN	**Odpovede**
Aký typ pripojenia vytvárate? • Hostiteľ-hostiteľ • Hostiteľ-brána • Brána-hostiteľ • Brána-brána	
Ako pomenujete pripojenie?	
Aký je identifikátor lokálneho koncového bodu pripojenia?	
Aký je identifikátor vzdialeného koncového bodu pripojenia?	
Aký je identifikátor lokálneho koncového bodu údajov?	
Aký je identifikátor vzdialeného koncového bodu údajov?	
Aký typ prenosu povolíte pre toto pripojenie (lokálny port, vzdialený port a protokol)?	
Vyžadujete preklad adries pre toto pripojenie? Pozrite si Preklad sieťových adries pre VPN, kde nájdete viac informácií.	
Budete používať tunelový režim alebo prenosový režim?	
Ktorý protokol IPSec bude pripojenie používať (AH, ESP alebo AH s ESP)? Pozrite si IPSec (IP Security), kde nájdete viac informácií.	
Ktorý autentifikačný algoritmus bude pripojenie používať (HMAC-MD5 alebo HMAC-SHA)?	
Ktorý šifrovací algoritmus bude pripojenie používať (DES-CBC alebo 3DES-CBC)? **Poznámka:** Šifrovací algoritmus zadajte, len ak ste vybrali ESP ako váš protokol IPSec.	
Aký je vstupný kľúč AH? Ak použijete MD5, kľúč je 16-bajtový hexadecimálny reťazec. Ak použijete SHA, kľúč je 20-bajtový hexadecimálny reťazec. Váš vstupný kľúč sa musí presne zhodovať s výstupným kľúčom vzdialeného servera.	
Aký je výstupný kľúč AH? Ak použijete MD5, kľúč je 16-bajtový hexadecimálny reťazec. Ak použijete SHA, kľúč je 20-bajtový hexadecimálny reťazec. Váš výstupný kľúč sa musí presne zhodovať so vstupným kľúčom vzdialeného servera.	
Aký je vstupný kľúč ESP? Ak použijete DES, kľúč je 8-bajtový hexadecimálny reťazec. Ak použijete 3DES, kľúč je 24-bajtový hexadecimálny reťazec. Váš vstupný kľúč sa musí presne zhodovať s výstupným kľúčom vzdialeného servera.	
Aký je výstupný kľúč ESP? Ak použijete DES, kľúč je 8-bajtový hexadecimálny reťazec. Ak použijete 3DES, kľúč je 24-bajtový hexadecimálny reťazec. Váš výstupný kľúč sa musí presne zhodovať so vstupným kľúčom vzdialeného servera.	

Tabuľka 12. Konfigurácia VPN (pokračovanie)

Aký je vstupný Index bezpečnostnej politiky (Security Policy Index, SPI)? Vstupný SPI je 4-bajtový hexadecimálny reťazec, kde prvý bajt je nastavený na 00. Váš vstupný SPI sa musí presne zhodovať s výstupným SPI vzdialeného servera.	
Aký je výstupný SPI? Výstupný SPI je 4-bajtový hexadecimálny reťazec. Váš výstupný SPI sa musí presne zhodovať so vstupným SPI vzdialeného servera.	

Súvisiace koncepty

"Preklad sieťových adries pre VPN" na strane 8
VPN poskytuje prostriedky na preklad sieťových adries nazývaný VPN NAT. VPN NAT sa líši od zvyčajného NAT v tom, že prekladá adresy pred použitím protokolov IKE a IPSec. Obráťte sa na túto tému, v ktorej sa dozviete viac.

Konfigurácia VPN

Rozhranie VPN vám ponúka niekoľko rôznych spôsobov na konfiguráciu vašich pripojení VPN. Môžete nakonfigurovať manuálne alebo dynamické pripojenie.

Dynamické pripojenie je to, ktoré kým je aktívne, dynamicky pomocou protokolu IKE (Internet Key Exchange) generuje a vyjednáva kľúče, ktorými je zabezpečované vaše pripojenie. Dynamické pripojenia poskytujú dodatočnú úroveň bezpečnosti údajov, ktoré nimi prechádzajú, lebo kľúče sa v pravidelných intervaloch automaticky menia. Následkom toho je menej pravdepodobné, že útočník zachytí kľúč, bude mať čas odhaliť ho a použiť ho na zneužitie alebo zachytenie prenosu, ktorý tieto kľúče ochraňujú.

Manuálne pripojenie naopak neposkytuje podporu vyjednávaniam IKE a v dôsledku toho ani automatickému riadeniu kľúčov. Okrem toho, oba konce pripojenia vyžadujú, aby ste nakonfigurovali niekoľko atribútov, ktoré sa musia presne zhodovať. Manuálne pripojenia používajú statické kľúče, ktoré sa neobnovujú ani nemenia, kým je pripojenie aktívne. Ak chcete zmeniť priradený kľúč manuálneho pripojenia, musíte ho zastaviť. Ak to považujete za bezpečnostné riziko, budete pravdepodobne chcieť radšej vytvoriť dynamické pripojenie.

Súvisiace koncepty

"Plánovanie VPN" na strane 40
Prvým krokom správneho používania VPN je plánovanie. Táto téma vám poskytne informácie o migrácii z predchádzajúcich vydaní, požiadavkách na inštaláciu a odkazy na plánovacieho poradcu, ktorý vygeneruje plánovaciu tabuľku prispôsobenú vašim špecifikáciám.

Konfigurácia pripojení VPN pomocou sprievodcu Nové pripojenie

Sprievodca Nové pripojenie umožňuje vytvoriť virtuálnu súkromnú sieť (VPN) medzi kombináciou hostiteľov a brán.

Napríklad hostiteľ-hostiteľ, brána-hostiteľ, hostiteľ-brána alebo brána-brána.

Sprievodca automaticky vytvorí každý z objektov konfigurácie, ktoré VPN vyžaduje pre svoju správnu činnosť, vrátane pravidiel pre pakety. Ak však vašej VPN potrebujete pridať nejaké funkcie, napríklad žurnálovanie siete alebo prekladanie sieťových adries VPN (VPN NAT), budete možno chcieť spresniť vašu VPN prostredníctvom listov vlastností príslušnej skupiny dynamických kľúčov alebo konkrétneho pripojenia. Za týmto účelom musíte najskôr zastaviť pripojenie, ak je aktívne. Potom kliknite pravým tlačidlom na skupinu alebo pripojenie dynamických kľúčov a vyberte **Vlastnosti**.

Na začiatku spustite poradcu plánovania pre VPN. Poradca zabezpečuje prostriedky na zhromažďovanie informácií nevyhnutných na vytvorenie svojej VPN.

Ak chcete vytvoriť VPN so sprievodcom Pripojenie, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.

2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu.
3. Dokončite sprievodcu a vytvoríte základné pripojenie VPN. Ak potrebujete pomoc, kliknite na **Pomoc**.

Súvisiace úlohy

Poradca pre plánovanie VPN

Konfigurácia bezpečnostných politík VPN

Keď určíte, ako budete používať vašu VPN, musíte definovať svoje bezpečnostné politiky VPN.

Poznámka: Po nakonfigurovaní vašich bezpečnostných politík VPN, musíte nakonfigurovať bezpečné pripojenia.

Súvisiace úlohy

"Konfigurácia zabezpečeného pripojenia VPN" na strane 47
Keď ste nakonfigurovali bezpečnostné politiky pre vaše pripojenie, potom musíte nakonfigurovať bezpečné pripojenie.

Konfigurácia politiky IKE (Internet Key Exchange)

Politika IKE (Internet Key Exchange) definuje, akú úroveň ochrany autentifikáciou a šifrovaním využíva IKE počas 1 fázy vyjednávania.

Fáza 1 IKE vytvorí kľúče, ktoré chránia správy, ktoré sa prenášajú v nasledujúcich vyjednávaniach fázy 2. Keď vytvoríte manuálne pripojenie, nemusíte definovať politiku IKE. Okrem toho, ak vytvoríte vašu VPN so sprievodcom Nové pripojenie, sprievodca môže vytvoriť vašu politiku IKE za vás.

VPN používa na autentifikáciu vyjednávaní fázy 1 buď podpisový režim RSA alebo dopredu zdieľané kľúče. Ak pri autentifikácii serverov kľúčov plánujete využívať digitálne certifikáty, musíte ich najprv nakonfigurovať pomocou Správca digitálnych certifikátov. Politika IKE tiež identifikuje, ktorý vzdialený server kľúčov bude používať túto politiku.

Ak chcete definovať politiku IKE alebo vykonať zmeny na existujúcej, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → IP Security Policies**.
2. Ak chcete vytvoriť novú politiku, kliknite pravým tlačidlom na **Politiky Internet Key Exchange** a vyberte **Nová politika Internet Key Exchange**. Ak chcete vykonať zmeny na existujúcej politike, v ľavom okne kliknite na **Politiky Internet Key Exchange**, potom v pravom okne kliknite pravým tlačidlom na politiku, ktorú chcete zmeniť a vyberte **Vlastnosti**.
3. Vyplňte všetky hárky vlastností. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Kliknutím na **OK** uložíte vaše zmeny.

Pri každom použití dopredu zdieľaného kľúča pre autentifikáciu sa odporúča použiť dohodovanie hlavného režimu. Poskytuje to bezpečnejšiu výmenu. Ak musíte používať dopredu zdieľané kľúče a agresívny režim dohodovania, vyberte skrytie hesiel, pre ktoré nebude jednoduché odhalenie pri narušení, ktoré skenuje slovník. Taktiež sa odporúča, aby ste si pravidelne menili svoje heslá. Na nanútenie hlavného režimu dohodovania pre výmenu kľúčov postupujte takto:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Vyberte **Budovanie VPN → Bezpečnostné politiky IP → Politiky Internet Key Exchange**, aby ste zobrazili aktuálne definované politiky výmeny kľúčov v pravej časti okna.
3. Pravým tlačidlom myši kliknite na konkrétnu politiku výmeny kľúčov a vyberte **Vlastnosti**.
4. Na stránke transformácií kliknite na **Odpovedajúca politika**. Objaví sa dialóg odpovedajúcej politiky internetovej výmeny kľúčov.
5. V poli Ochrana identity zrušte výber **Agresívny režim dohodovania IKE (bez ochrany identity).**
6. Kliknutím na **OK** sa vrátite do dialógového okna Vlastnosti.
7. Opätovným kliknutím na **OK** uložíte vaše zmeny.

Poznámka: Po nastavení poľa ochrany identifikácie sa zmena prejaví pre všetky výmeny so vzdialenými kľúčovými servermi, pretože pre celý systém existuje len jedna odpovedajúca politika IKE. Hlavný režim dohodovania zabezpečí, že spúšťací systém môže vyžadovať len hlavný režim výmeny politík kľúčov.

Súvisiace koncepty

"Správa kľúčov" na strane 6
Dynamická VPN zabezpečuje dodatočnú bezpečnosť pre vašu komunikáciu pomocou protokolu Internet Key Exchange (IKE) pre správu kľúčov. IKE umožňuje VPN serverom na oboch koncoch pripojenia vyjednávať v určených intervaloch nové kľúče.

Súvisiace úlohy

Správca digitálnych certifikátov

Konfigurácia údajovej politiky

Údajová politika definuje, aká úroveň autentifikácie alebo šifrovania ochraňuje údaje počas ich prenosu cez VPN.

Komunikačné systémy sa dohodnú na týchto atribútoch počas vyjednávaní fázy 2 protokolu Internet Key Exchange (IKE). Keď vytvoríte manuálne pripojenie, nemusíte definovať údajovú politiku. Okrem toho, ak vytvoríte vašu VPN so sprievodcom Nové pripojenie, sprievodca môže vytvoriť vašu údajovú politiku za vás.

Ak chcete definovať údajovú politiku alebo vykonať zmeny na existujúcej, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → IP Security Policies**.
2. Ak chcete vytvoriť novú údajovú politiku, kliknite pravým tlačidlom na **Politiky údajov** a vyberte **Nová údajová politika**. Ak chcete vykonať zmeny na existujúcej údajovej politike, kliknite na **Politiky údajov** (v ľavom okne), potom kliknite pravým tlačidlom na údajovú politiku, ktorú chcete zmeniť (v pravom okne) a vyberte **Vlastnosti**.
3. Vyplňte všetky hárky vlastností. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Kliknutím na **OK** uložíte vaše zmeny.

Súvisiace koncepty

"Správa kľúčov" na strane 6
Dynamická VPN zabezpečuje dodatočnú bezpečnosť pre vašu komunikáciu pomocou protokolu Internet Key Exchange (IKE) pre správu kľúčov. IKE umožňuje VPN serverom na oboch koncoch pripojenia vyjednávať v určených intervaloch nové kľúče.

Konfigurácia zabezpečeného pripojenia VPN

Keď ste nakonfigurovali bezpečnostné politiky pre vaše pripojenie, potom musíte nakonfigurovať bezpečné pripojenie.

Pre dynamické pripojenia obsahuje objekt bezpečnostného pripojenia skupinu dynamických kľúčov a pripojenie dynamických kľúčov.

Skupina dynamických kľúčov definuje bežné charakteristiky jedného alebo viacerých pripojení VPN. Konfigurácia skupiny dynamických kľúčov umožňuje pre každé pripojenie v skupine používať rovnaké politiky, ale rôzne koncové body údajov. Skupiny dynamických kľúčov úspešne vyjednávajú so vzdialenými iniciátormi, keď koncové body údajov navrhnuté vzdialeným systémom, nie sú konkrétne dopredu známe. Vykoná to priradením informácií o politike v skupine dynamických kľúčov k pravidlu pre filtre politiky s typom akcie IPSEC. Ak špecifické koncové body údajov, ktoré ponúkol vzdialený iniciátor, sú v rozmedzí určenom v pravidle pre filtre IPSEC, môžu podliehať politike definovanej v skupine dynamických kľúčov.

Pripojenie dynamických kľúčov definuje charakteristiky jednotlivých údajových pripojení medzi dvojicami koncových bodov. Pripojenie dynamických kľúčov existuje v skupine dynamických kľúčov. Po nakonfigurovaní skupiny dynamických kľúčov opisujúcej, ktoré pripojenia politiky sa majú v skupine použiť, potrebujete vytvoriť individuálne pripojenia dynamických kľúčov pre pripojenia, ktoré ste nainicializovali lokálne.

Ak chcete konfigurovať objekt bezpečného pripojenia, vykonajte úlohy z Časti 1 aj 2:

Súvisiace koncepty

"Konfigurácia bezpečnostných politík VPN" na strane 46
Keď určíte, ako budete používať vašu VPN, musíte definovať svoje bezpečnostné politiky VPN.

"Konfigurácia pravidiel pre pakety VPN" na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Súvisiace úlohy

"Aktivácia pravidiel pre pakety VPN" na strane 53
Pred spustením pripojenia VPN aktivujte pravidlá pre pakety VPN.

Časť 1: Konfigurácia skupiny dynamických kľúčov

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP → Virtuálne súkromné siete → Bezpečné pripojenia**.
2. Pravým tlačidlom myši kliknite na **Podľa skupiny** a vyberte **Nová skupina dynamických kľúčov**.
3. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Kliknutím na **OK** uložíte vaše zmeny.

Časť 2: Konfigurácia pripojenia dynamických kľúčov

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections → By Group**.
2. V ľavej časti okna System i Navigator pravým tlačidlom myši kliknite na skupinu dynamických kľúčov, ktorú ste vytvorili v časti 1 a vyberte **Nové pripojenie dynamických kľúčov**.
3. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Kliknutím na **OK** uložíte vaše zmeny.

Po vykonaní týchto krokov musíte aktivovať pravidlá pre pakety, ktoré pripojenie vyžaduje na svoju prevádzku.

Poznámka: Vo väčšine prípadov môžete vybrať voľbu **Vygenerovať nasledujúci filter politiky pre túto skupinu** na strane **Skupina dynamických kľúčov - Pripojenia**, aby ste rozhraniu VPN povolili automatické generovanie vašich pravidiel pre pakety VPN. Ak však vyberiete voľbu **Pravidlo pre filtre politiky bude definované v Pravidlách pre pakety**, musíte nakonfigurovať pravidlá pre pakety VPN pomocou editora Pravidiel pre pakety a potom ich aktivovať.

Konfigurácia manuálneho pripojenia

Manuálne pripojenie je pripojenie, pri ktorom musíte nakonfigurovať všetky vlastnosti vašej VPN bez využitia akýchkoľvek sprievodcov.

Okrem toho, oba konce pripojenia vyžadujú, aby ste nakonfigurovali niekoľko prvkov, ktoré sa musia *presne* zhodovať. Napríklad vstupné kľúče sa musia zhodovať s výstupnými kľúčmi vzdialeného systému, inak pripojenie zlyhá.

Manuálne pripojenia používajú statické kľúče, ktoré sa neobnovujú ani nemenia, kým je pripojenie aktívne. Ak chcete zmeniť priradený kľúč manuálneho pripojenia, musíte ho zastaviť. Ak to považujete za bezpečnostné riziko a ak oba konce pripojenia podporujú protokol IKE (Internet Key Exchange), mali by ste pravdepodobne zvážiť možnosť nastavenie dynamického pripojenia.

Ak chcete definovať vlastnosti pre svoje manuálne pripojenie, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → → Secure Connections**.
2. Kliknite pravým tlačidlom na **Všetky pripojenia** a vyberte **Nové manuálne pripojenie**.
3. Vyplňte všetky hárky vlastností. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.

4. Kliknutím na **OK** uložíte vaše zmeny.

Poznámka: Vo väčšine prípadov môžete vybrať voľbu **Vygenerovať filter politiky, ktorý zodpovedá koncovým bodom údajov** na strane **Manuálne pripojenie - Pripojenie**, aby ste rozhraniu VPN povolili automatické generovanie vašich pravidiel pre pakety VPN. Ak však vyberiete voľbu **Pravidlo pre filtre politiky bude definované v Pravidlách pre pakety**, pravidlo pre filtre politiky musíte nakonfigurovať manuálne a potom politiky aktivovať.

Súvisiace úlohy

"Konfigurácia pravidla filtrovania politiky" na strane 51
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

Konfigurácia dynamického pripojenia

Kým je dynamické pripojenie aktívne, pomocou protokolu IKE (Internet Key Exchange) dynamicky generuje a vyjednáva kľúče, ktorými je zabezpečované vaše pripojenie.

Nasledujúcimi krokmi vyplníte údaje v sprievodcovi New Dynamic-Key Connection a nakonfigurujete dynamické pripojenie:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections → By Group**.
2. Kliknite pravým tlačidlom myši na konkrétnu skupinu dynamických kľúčov a vyberte **New Dynamic-Key Connection**.
3. Vyplňte všetky hárky vlastností. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Kliknutím na **OK** uložíte vaše zmeny.

Konfigurácia pravidiel pre pakety VPN

Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Ak chcete vytvoriť pravidlá pre pakety VPN pomocou editora Pravidiel pre pakety v System i Navigator, vytvorte všetky dodatočné pravidlá týmto spôsobom. Naopak, ak vaše pravidlá filtrovania politiky vygenerovala VPN, vytvorte všetky dodatočné pravidlá filtrovania politiky týmto spôsobom.

Vo všeobecnosti VPN vyžadujú dva typy pravidiel pre filtre: pravidlá pre filtre Pre-IPSec a pravidlá pre filtre politiky. Pozrite si témy uvedené nižšie, aby ste sa oboznámili so spôsobom konfigurácie týchto pravidiel pomocou editora Pravidiel pre pakety v System i Navigator. Ak chcete získať informácie o iných voľbách VPN a filtrovania, pozrite si časť VPN a filtrovanie IP v téme Koncepty VPN.

- Konfigurácia pravidiel pre filtre pre-IPSec

  Pravidlá pre-IPSec sú všetky pravidlá vo vašom systéme, ktoré budú pred pravidlami s typom akcie IPSEC. Táto téma opisuje len pravidlá pre-IPSec, ktoré VPN vyžaduje pre svoju správnu činnosť. V takomto prípade pravidlá pre-IPSec sú dvojice pravidiel, ktoré povoľujú spracovávanie IKE cez pripojenie. IKE umožňuje pre vaše pripojenie generovanie dynamických kľúčov a vyjednávania. V závislosti na vašom sieťovom prostredí a bezpečnostnej politike možno budete chcieť pridať ďalšie pravidlá pre-IPSec.

  Poznámka: Ak máte pravidlá, ktoré povoľujú IKE pre špecifické systémy, musíte nakonfigurovať už len tento typ pravidla pre-IPSec. Ak nie sú na systéme napísané žiadne filtrovacie pravidlá na povolenie prenosu IKE, potom je prenos IKE implicitne povolený.

- Nakonfigurovať pravidlo pre filtre politiky

  Pravidlo pre filtre politiky definuje prenos, ktorý môže používať VPN a aká politika ochrany údajov sa má použiť na tento prenos.

Úvodné záležitosti na zváženie

Keď pridáte pravidlá pre filtre do rozhrania, systém automaticky pridá pre toto rozhranie predvolené pravidlo DENY. Znamená to, že sa zakáže všetok prenos, ktorý nie je výslovne dovolený. Toto pravidlo nemôžete vidieť ani zmeniť. Následkom toho sa môže stať, že prenosy, ktoré predtým fungovali, budú po aktivácii vašich pravidiel pre pakety záhadne zlyhávať. Ak chcete na rozhraní povoliť iný prenos ako VPN, musíte pridať výslovné pravidlá PERMIT.

Po konfigurácii príslušných filtrovacích pravidiel musíte definovať rozhranie, na ktoré budú použité a potom ich musíte aktivovať.

Je nevyhnutné, aby ste svoje pravidlá pre filtre správne nakonfigurovali. Ak to nespravíte, filtrovacie pravidlá môžu blokovať celú prichádzajúcu a odchádzajúcu premávku IP z vášho systému. Toto zahrňuje vaše pripojenie k System i Navigator, ktoré používate na konfiguráciu filtrovacích pravidiel.

Ak pravidlá filtrovania nepovoľujú prenosy System i, nemôže System i Navigator komunikovať s vaším systémom. Ak dôjde k tomuto, prihláste sa do vášho systému pomocou rozhrania, ktoré sa dokáže pripojiť, napríklad Operačnej konzoly. Na odstránenie všetkých filtrov na tomto systéme použite príkaz RMVTCPTBL. Tento príkaz tiež ukončí všetky servery *VPN a potom ich reštartuje. Potom nakonfigurujte svoje filtre a znova ich aktivujte.

Súvisiace koncepty

“Filtrovanie VPN a IP” na strane 11
Filtrovanie IP a VPN spolu tesne súvisia. V skutočnosti väčšina pripojení VPN vyžaduje, aby pravidlá pre filtre pracovali správne. Táto téma poskytuje informácie o tom, čo vyžadujú filtre VPN, ako aj ostatné koncepty filtrovania súvisiace s VPN.

Súvisiace úlohy

“Konfigurácia zabezpečeného pripojenia VPN” na strane 47
Keď ste nakonfigurovali bezpečnostné politiky pre vaše pripojenie, potom musíte nakonfigurovať bezpečné pripojenie.

“Konfigurácia pravidiel pre filtre pre-IPSec”
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

“Konfigurácia pravidla filtrovania politiky” na strane 51
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

“Definovanie rozhrania pravidiel filtrovania VPN” na strane 52
Keď ste nakonfigurovali svoje pravidlá pre pakety VPN a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré sa použijú.

“Aktivácia pravidiel pre pakety VPN” na strane 53
Pred spustením pripojenia VPN aktivujte pravidlá pre pakety VPN.

Konfigurácia pravidiel pre filtre pre-IPSec

Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

Dvojica serverov Internet Key Exchange (IKE) dynamicky vyjednáva a obnovuje kľúče. IKE používa známy port 500. Aby IKE pracovala správne, musíte povoliť datagramy UDP cez port 500 pre tento prenos IP. Za týmto účelom vytvoríte dvojicu pravidiel pre filtre. Jedno pre prichádzajúci prenos a jedno pre odchádzajúci prenos, takže vaše pripojenie bude môcť dynamicky vyjednávať kľúče na ochranu pripojenia:

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Týmto otvoríte editor Pravidiel pre pakety, ktorý vám umožňuje vytvoriť alebo upraviť pravidlá pre filtre a NAT pre váš systém.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore Pravidlá paketov vyberte **Insert → Filter**.

5. Na stránke **Všeobecné** zadajte názov množiny pre vaše pravidlá pre filtre VPN. Odporúča sa, aby ste si vytvorili minimálne tri odlišné sady: jednu pre filtrovacie pravidlá pre-IPSec, jednu pre filtrovacie pravidlá politiky a jednu pre rôzne filtrovacie pravidlá PERMIT a DENY. Pomenujte sadu obsahujúcu filtrovacie pravidlá pre-IPSec s predponou *preipsec*. Napríklad preipsecfiltre.
6. V poli **Akcia** z rozbaľovacieho zoznamu vyberte **PERMIT**.
7. V poli **Smer** z rozbaľovacieho zoznamu vyberte **OUTBOUND**.
8. V poli **Názov zdrojovej adresy** z rozbaľovacieho zoznamu vyberte **=** a do druhého poľa zadajte adresu IP lokálneho servera kľúčov. Zadali ste adresu IP lokálneho servera kľúčov v politike IKE.
9. V poli **Názov cieľovej adresy** z rozbaľovacieho zoznamu vyberte **=** a do druhého poľa zadajte adresu IP vzdialeného servera kľúčov. Takisto ste zadali adresu IP vzdialeného servera kľúčov v politike IKE.
10. Na stránke **Služby** vyberte **Služba**. Takto umožníte polia **Protokol**, **Port zdroja** a **Port cieľa**.
11. V poli **Protokol** z rozbaľovacieho zoznamu vyberte **UDP**.
12. Pre **Port cieľa** v prvom poli vyberte **=** a v druhom poli zadajte 500.
13. Zopakujte predchádzajúci krok pre **Port cieľa**.
14. Kliknite na **OK**.
15. Zopakujte tieto kroky na konfiguráciu filtra INBOUND. Podľa potreby použite rovnaký názov množiny a obrátené adresy.

Poznámka: Menej bezpečná, ale jednoduchšia možnosť na povolenie premávky IKE cez toto pripojenie, je nakonfigurovať len jeden filter pre pre-IPSec a použiť zástupné znaky (*) v poliach **Smer**, **Názov zdrojovej adresy** a **Názov cieľovej adresy**.

Ďalším krokom je konfigurácia pravidla pre filtre politiky, v ktorom môžete definovať premávku IP, ktorú má ochraňovať pripojenie VPN.

Súvisiace koncepty

“Konfigurácia pravidiel pre pakety VPN” na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Súvisiace úlohy

“Konfigurácia pravidla filtrovania politiky”
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

Konfigurácia pravidla filtrovania politiky

Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

Pravidlo pre filtre politiky (pravidlo, kde action=IPSEC) definuje, ktoré adresy, protokoly a porty môžu používať VPN. Definuje aj politiku, ktorá sa použije na prenos v pripojení VPN. Ak chcete nakonfigurovať pravidlo pre filtre politiky, postupujte podľa týchto krokov:

Poznámka: Ak ste práve nakonfigurovali pravidlo pre pre-IPSec (len pre dynamické pripojenia), editor Pravidiel pre pakety bude stále otvorený; prejdite na krok 4.

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Týmto otvoríte editor Pravidiel pre pakety, ktorý vám umožňuje vytvoriť alebo upraviť pravidlá pre filtre a NAT pre váš systém.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore Pravidlá paketov vyberte **Insert → Filter**.

5. Na stránke **Všeobecné** zadajte názov množiny pre vaše pravidlá pre filtre VPN. Odporúča sa, aby ste si vytvorili minimálne tri odlišné sady: jednu pre filtrovacie pravidlá pre-IPSec, jednu pre filtrovacie pravidlá politiky a jednu pre rôzne filtrovacie pravidlá PERMIT a DENY. Napríklad filtrepolitiky
6. V poli **Akcia** z rozbaľovacieho zoznamu vyberte **IPSEC**. Pole **Smer** štandardne obsahuje OUTBOUND a nemôžete ho zmeniť. Hoci je toto pole štandardne nastavené na OUTBOUND, v skutočnosti je obojsmerné. Zobrazené je ako OUTBOUND na objasnenie sémantiky vstupných hodnôt. Napríklad zdrojové hodnoty sú lokálne hodnoty a cieľové hodnoty sú vzdialené hodnoty.
7. Pre **Názov zdrojovej adresy** v prvom poli vyberte **=** a v druhom poli zadajte adresu IP lokálneho koncového bodu údajov. Môžete tiež zadať rozsah adries IP alebo adresu IP a masku podsiete po tom, ako ich nakonfigurujete pomocou funkcie **Definovať adresy**.
8. Pre **Názov cieľovej adresy** v prvom poli vyberte **=** a v druhom poli zadajte adresu IP vzdialeného koncového bodu údajov. Môžete tiež zadať rozsah adries IP alebo adresu IP a masku podsiete po tom, ako ich nakonfigurujete pomocou funkcie **Definovať adresy**.
9. V poli **Žurnálovanie** zadajte, ktorú úroveň žurnálovania vyžadujete.
10. V poli **Názov pripojenia** vyberte definíciu pripojenia, na ktorú sa použijú tieto filtre.
11. (voliteľné) Zadajte popis.
12. Na stránke **Služby** vyberte **Služba**. Takto umožníte polia **Protokol**, **Port zdroja** a **Port cieľa**.
13. V poliach **Protokol**, **Zdrojový port** a **Cieľový port** vyberte príslušné hodnoty pre premávku. Alebo z rozbaľovacieho zoznamu môžete vybrať hviezdičku (*). Takto ktorémukoľvek protokolu používajúcemu ktorýkoľvek port povolíte používať VPN.
14. Kliknite na **OK**.

Ďalším krokom je definovanie rozhrania, na ktoré budú aplikované tieto pravidlá.

Poznámka: Ak pridáte filtrovacie pravidlá do rozhrania, systém automaticky pridá pre toto rozhranie predvolené pravidlo DENY. Znamená to, že sa zakáže všetok prenos, ktorý nie je výslovne dovolený. Toto pravidlo nemôžete vidieť ani zmeniť. Následkom toho sa môže stať, že pripojenie, ktoré predtým fungovalo, po aktivácii pravidiel filtrovania záhadne zlyhá. Ak chcete na rozhraní povoliť iný prenos ako VPN, musíte pridať výslovné pravidlá PERMIT.

Súvisiace koncepty

“Konfigurácia pravidiel pre pakety VPN” na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Súvisiace úlohy

“Konfigurácia manuálneho pripojenia” na strane 48
Manuálne pripojenie je pripojenie, pri ktorom musíte nakonfigurovať všetky vlastnosti vašej VPN bez využitia akýchkoľvek sprievodcov.

“Konfigurácia pravidiel pre filtre pre-IPSec” na strane 50
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

“Definovanie rozhrania pravidiel filtrovania VPN”
Keď ste nakonfigurovali svoje pravidlá pre pakety VPN a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré sa použijú.

Definovanie rozhrania pravidiel filtrovania VPN

Keď ste nakonfigurovali svoje pravidlá pre pakety VPN a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré sa použijú.

Ak chcete definovať rozhranie, na ktoré použiť vaše pravidlá pre filtre VPN, postupujte podľa týchto krokov:

Poznámka: Ak ste práve nakonfigurovali pravidlá pre pakety VPN, rozhranie Pravidiel pre pakety bude stále otvorené; prejdite na krok 4.

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Týmto otvoríte editor Pravidiel pre pakety, ktorý vám umožňuje vytvoriť alebo upraviť pravidlá pre filtre a NAT pre váš systém.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore Pravidlá paketov vyberte **Insert → Filter Interface**.
5. Na stránke **Všeobecné** vyberte **Názov linky**, potom z rozbaľovacieho zoznamu vyberte popis linky, na ktorú sa použijú vaše pravidlá pre pakety VPN.
6. (voliteľné) Zadajte popis.
7. Na stránke **Množiny filtrov** kliknutím na **Pridať** pridáte každý názov množiny pre filtre, ktoré ste práve nakonfigurovali.
8. Kliknite na **OK**.
9. Uložte svoj súbor s pravidlami. Súbor bude uložený do integrovaného súborového systému vo vašom systéme s rozšírením .i3p.

   Poznámka: Tento súbor neuchovávajte do tohto adresára:

   `/QIBM/UserData/OS400/TCPIP/RULEGEN`

   Tento adresár je len pre systémové použitie. Keby ste niekedy potrebovali použiť príkaz RMVTCPTBL *ALL na deaktiváciu pravidiel pre pakety, tento príkaz vymaže všetky súbory v tomto adresári.

Po zadefinovaní rozhrania pre vaše filtrovacie pravidlá musíte pred spustením VPN tieto pravidlá aktivovať.

Súvisiace koncepty

"Konfigurácia pravidiel pre pakety VPN" na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Súvisiace úlohy

"Konfigurácia pravidla filtrovania politiky" na strane 51
Vykonajte túto úlohu len v prípade, ak ste špecifikovali, že nechcete, aby VPN automaticky generovalo pravidlo pre filtre politiky.

"Aktivácia pravidiel pre pakety VPN"
Pred spustením pripojenia VPN aktivujte pravidlá pre pakety VPN.

Aktivácia pravidiel pre pakety VPN

Pred spustením pripojenia VPN aktivujte pravidlá pre pakety VPN.

Ak máte na vašom systéme spustené pripojenia VPN, nemôžete aktivovať (alebo deaktivovať) spomínané pravidlá. Kým aktivujete pravidlá pre filtre VPN, skontrolujte, či neexistujú žiadne s nimi spojené aktívne pripojenia.

Ak ste vytvorili pripojenie VPN so sprievodcom Nové pripojenie, zvoľte, aby sa priradené pravidlá aktivovali automaticky. Vezmite do úvahy, že ak sú na ktoromkoľvek z rozhraní, ktoré ste zadali, aktívne iné pravidlá pre pakety, nahradia ich pravidlá pre filtre politiky VPN.

Ak si vyberiete aktiváciu VPN generovaných pravidiel použitím editora pravidiel pre pakety, postupujte takto:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Aktivovať**. Toto otvorí dialógové okno **Aktivovať pravidlá pre pakety**.
3. Vyberte, či chcete aktivovať len vygenerované pravidlá VPN, len vybraný súbor alebo aj vygenerované pravidlá VPN aj vybraný súbor. Druhú možnosť môžete vybrať, ak napríklad máte rôznorodé pravidlá PERMIT a DENY, ktoré chcete vynútiť na rozhraní okrem vygenerovaných pravidiel VPN.

4. Vyberte rozhranie, na ktorom chcete aktivovať pravidlá. Možno zvoliť aktiváciu na určitom rozhraní, na identifikátore typu point-to-point alebo na všetkých identifikátoroch typu point-to-point.
5. V dialógovom okne kliknite na **OK**, čím potvrdíte, že si želáte overiť a aktivovať pravidlá na zadaných rozhraniach. Keď kliknete na OK, systém skontroluje pravidlá pre syntaktické a sémantické chyby ohlási výsledky v okne správy v spodnej časti editora. Chybové správy, ktoré sú spojené s určitým súborom a číslom riadka, získate, keď kliknete pravým tlačidlom na chybu a vyberiete **Prejsť na riadok**, čím zvýrazníte chybu v súbore.

Po aktivácii vašich pravidiel filtrovania môžete spustiť pripojenie VPN.

Súvisiace koncepty

"Konfigurácia pravidiel pre pakety VPN" na strane 49
Ak vytvárate pripojenie prvýkrát, povoľte, aby vám VPN automaticky vygenerovala pravidlá pre pakety VPN. Toto vykonáte buď pomocou sprievodcu Nové pripojenie alebo stránok s vlastnosťami VPN na konfiguráciu vášho pripojenia.

Súvisiace úlohy

"Konfigurácia zabezpečeného pripojenia VPN" na strane 47
Keď ste nakonfigurovali bezpečnostné politiky pre vaše pripojenie, potom musíte nakonfigurovať bezpečné pripojenie.

"Definovanie rozhrania pravidiel filtrovania VPN" na strane 52
Keď ste nakonfigurovali svoje pravidlá pre pakety VPN a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré sa použijú.

"Spustenie pripojenia VPN" na strane 55
Pomocou tejto úlohy spustíte pripojenia, ktoré sa zahajujú lokálne.

Konfigurácia utajenia toku prenosov

Ak máte nakonfigurovanú údajovú politiku tunelového režimu, môžete na utajenie skutočnej dĺžky údajových paketov prenášaných prostredníctvom pripojenia VPN využívať utajenie toku prenosov (TFC).

TFC pridáva dodatočnú výplň do odosielaných paketov a odosiela umelé pakety s rôznymi dĺžkami v náhodných intervaloch, aby utajilo aktuálnu dĺžku týchto paketov. TFC použite, ak chcete získať dodatočnú bezpečnosť pred útočníkmi, ktorí môžu uhádnuť typ prenášaných údajov z dĺžky paketu. Ak aktivujete TFC, získate väčšiu bezpečnosť, ale za cenu zníženia výkonu systému. Preto najprv otestujte výkon vášho systému a až potom aktivujte TFC v pripojení VPN. IKE nedohoduje TFC a užívatelia by ho mali aktivovať, len ak ho podporujú oba systémy.

Ak chcete aktivovať TFC v pripojení VPN, vykonajte tieto kroky:

1. V System i Navigator rozviňte váš server>**Network → IP Policies → Virtual Private Networking → Secure Connections → All Connections**.
2. Pravým tlačidlom myši kliknite na pripojenie, ktorému chcete aktivovať TFC a vyberte **Vlastnosti**.
3. Na záložke **Všeobecné** vyberte **Použiť TFC (Traffic Flow Confidentiality) v režime tunela**.

Konfigurácia ESN (Extended Sequence Number)

Pomocou ESN (Extended Sequence Number) môžete zvýšiť prenosovú rýchlosť údajov pripojenia VPN.

Ak používate protokol AH alebo protokol ESP a ako šifrovací algoritmus používate AES, môžete povoliť ESN. ESN vám umožňuje prenášať veľký rozsah údajov vysokými rýchlosťami bez nutnosti prekľúčovania. Pripojenie VPN používa 64-bitové poradové čísla namiesto 32-bitových čísel cez protokol IPSec. Pri použití 64-bitových poradových čísel nie je potreba častého prekľúčovania, čím sa predchádza vyčerpaniu poradových čísel a minimalizuje sa používanie systémových prostriedkov.

Ak chcete povoliť ESN v pripojení VPN, vykonajte tieto kroky:

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP → Virtuálne súkromné siete**.
2. Pravým tlačidlom myši kliknite na **Budovanie VPN** a vyberte **Vlastnosti**.
3. Na záložke **Všeobecné** vyberte **Používať ESN (Extended Sequence Number)**.

Spustenie pripojenia VPN

Pomocou tejto úlohy spustíte pripojenia, ktoré sa zahajujú lokálne.

Tieto inštrukcie predpokladajú, že máte vaše pripojenie VPN správne nakonfigurované. Ak chcete spustiť vaše pripojenie VPN, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Ak nie je server VPN spustený, kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Spustiť**.
3. Skontrolujte, že pravidlá pre pakety sú aktivované.
4. Rozviňte **Budovanie VPN → Bezpečné pripojenia**.
5. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
6. Kliknite pravým tlačidlom na pripojenie, ktoré chcete spustiť a vyberte **Spustiť**. Ak chcete spustiť viac pripojení, vyberte všetky pripojenia, ktoré chcete spustiť a vyberte **Spustiť**.

Súvisiace úlohy

"Aktivácia pravidiel pre pakety VPN" na strane 53
Pred spustením pripojenia VPN aktivujte pravidlá pre pakety VPN.

"Začíname s odstraňovaním problémov s VPN" na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Riadenie VPN

Pomocou rozhrania VPN v System i Navigator môžete zvládnuť všetky vaše úlohy riadenia VPN, ako napríklad zastavenie pripojenia a zobrazenie atribútov pripojenia.

Rozhranie VPN v System i Navigator použite na vykonanie všetkých riadiacich úloh, vrátane:

Nastavenie predvolených atribútov vášho pripojenia

Predvolené hodnoty pochádzajú z panelov, ktoré používate na vytváranie nových politík a pripojení. Môžete nastaviť predvolené hodnoty pre úrovne bezpečnosti, správu relácií kľúčov, doby existencie kľúčov a doby existencie pripojení.

Keď na začiatku vytvoríte nové objekty VPN, predvolené bezpečnostné hodnoty vyplnia rôzne polia.

Ak chcete nastaviť predvolené bezpečnostné hodnoty pre vaše pripojenia VPN, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Sieť → Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Predvolené hodnoty**.
3. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
4. Po dokončení všetkých listov vlastností kliknite na **OK**.

Resetovanie pripojenia v chybovom stave

Resetovanie chybných pripojení ich navráti do stavu nečinnosti.

Ak chcete obnoviť pripojenie, ktoré je v chybovom stave, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Kliknite pravým tlačidlom na pripojenie, ktoré chcete resetovať a vyberte **Resetovať**. Takto resetujete pripojenie do stavu nečinnosti. Ak chcete resetovať viacero pripojení, ktoré sú v chybovom stave, vyberte všetky pripojenia, ktoré chcete resetovať kliknite pravým tlačidlom a vyberte **Resetovať**.

Zobrazovanie informácií o chybách

Táto úloha vám pomôže pri zisťovaní, prečo dochádza k chybe vo vašom pripojení.

Ak chcete zobraziť informácie o chybných pripojeniach, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Kliknite pravým tlačidlom na chybné pripojenie, ktoré chcete zobraziť a vyberte **Informácie o chybách**.

Súvisiace úlohy

"Začíname s odstraňovaním problémov s VPN" na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Zobrazenie atribútov aktívnych pripojení

Vykonajte túto úlohu na kontrolu stavu a iných atribútov vašich aktívnych pripojení.

Ak chcete zobraziť aktuálne atribúty aktívneho pripojenia alebo pripojenia na požiadanie, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Pravým tlačidlom myši kliknite na aktívne pripojenie alebo pripojenie na požiadanie, ktoré chcete zobraziť a vyberte **Vlastnosti**.
4. Prejdite na stránku **Aktuálne atribúty** a uvidíte atribúty pripojenia.

Atribúty všetkých pripojení môžete zobraziť z okna System i Navigator. Štandardne sa zobrazia len atribúty Stav, Popis a Typ pripojenia. Môžete zmeniť, ktoré údaje sa budú zobrazovať, keď budete postupovať podľa nasledujúcich krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Z ponuky **Objekty** vyberte **Stĺpce**. Otvorí sa dialógové okno, kde môžete vybrať atribúty, ktoré chcete zobraziť v okne System i Navigator.

Uvedomte si, že keď zmeníte stĺpce na zobrazenie, zmeny nie sú špecifické pre konkrétneho užívateľa alebo PC, ale sú skôr celosystémové.

Súvisiace koncepty

"Chybové správy Správcu pripojení VPN" na strane 70
Ak pri pripojení VPN dôjde k nejakej chybe, zaprotokoluje Správca pripojenia VPN v protokole úlohy QTOVMAN dve správy.

Zobrazenie sledovania servera VPN

Umožňuje vám konfigurovať, spustiť, zastaviť a zobraziť sledovania servera Správcu pripojení VPN a Správcu kľúčov VPN. Toto je podobné, ako používanie príkazu TRCTCPAPP *VPN zo znakového rozhrania. Odlišnosť je v tom, že si môžete sledovanie prezerať aj pri aktívnom spojení.

Ak chcete zobraziť sledovanie servera VPN, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Pravým tlačidlom myši kliknite na **Budovanie VPN**, vyberte **Diagnostické nástroje** a potom **Sledovanie servera**.

Ak chcete určiť typ sledovania, ktorý chcete, aby Správca kľúčov VPN a Správca pripojení VPN generovali, postupujte podľa týchto krokov:

1. V okne **Sledovanie virtuálnych súkromných sietí** kliknite na  (Voľby).
2. Na stránke **Správca pripojení** zadajte, aký typ sledovania chcete, aby server Správcu pripojení spustil.
3. Na strane **Správca kľúčov** zadajte typ sledovania, ktorý chcete, aby spustil server Správcu kľúčov.
4. Kliknite na **Pomoc**, ak máte akékoľvek otázky o vyplnení strany alebo ľubovoľného z jej polí.
5. Kliknutím na **OK** uložíte vaše zmeny.
6. Kliknite na  (Spustiť), aby ste spustili sledovanie. Pravidelným kliknutím na  (Obnoviť) zobrazte najaktuálnejšie informácie o sledovaní.

Zobrazenie protokolov úloh servera VPN

Podľa týchto inštrukcií zobrazíte protokoly úloh pre Správcu kľúčov VPN a Správcu pripojení VPN.

Ak chcete zobraziť aktuálne protokoly úloh buď Správcu kľúčov VPN alebo Správcu pripojení VPN, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete**, vyberte **Diagnostické nástroje** a potom vyberte ktorýkoľvek protokol úloh servera, ktorý chcete zobraziť.

Zobrazenie atribútov Bezpečnostných asociácií (SA)

Pomocou tejto úlohy zobrazíte atribúty Bezpečnostných asociácií (SA), ktoré sú priradené k povolenému pripojeniu.

Ak chcete zobraziť atribúty Bezpečnostných asociácií SA), ktoré sú priradené k povolenému pripojeniu. Za týmto účelom postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Pravým tlačidlom myši kliknite na príslušné aktívne pripojenie a vyberte **Bezpečnostné priradenia**. Výsledné okno vám umožní zobraziť vlastnosti každého bezpečného priradenia SA priradeného k špecifickému pripojeniu.

Zastavenie pripojenia VPN

Pomocou tejto úlohy zastavíte aktívne pripojenia.

Ak chcete zastaviť aktívne pripojenie alebo pripojenie na požiadanie, postupujte podľa týchto krokov:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Kliknite pravým tlačidlom na pripojenie, ktoré chcete zastaviť a vyberte **Zastaviť**. Ak chcete zastaviť viac pripojení, vyberte všetky pripojenia, ktoré chcete zastaviť a vyberte **Zastaviť**.

Vymazanie konfiguračných objektov VPN

Než vymažete objekt konfigurácie VPN z databázy politík VPN, uistite sa, či rozumiete tomu, ako to ovplyvní ostatné pripojenia a skupiny pripojení VPN.

Ak ste si istí, že chcete vymazať pripojenie VPN z databázy politík VPN, vykonajte nasledovné kroky:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.

3. Kliknite pravým tlačidlom na pripojenie, ktoré chcete vymazať a vyberte **Vymazať**.

Odstraňovanie problémov s VPN

Pomocou nasledujúcich metód odstraňovania problémov môžete riešiť niektoré zo základných problémov, ktoré by ste mohli zaznamenať počas konfigurácie pripojenia VPN.

VPN je zložitá a rýchlo sa meniaca technológia, ktorá vyžaduje aspoň základné znalosti štandardných technológií IPSec. Tiež vám musia byť známe pravidlá pre pakety IP, pretože VPN vyžaduje pre správne fungovanie niekoľko filtrovacích pravidiel. Vzhľadom na komplexnosť týchto informácií sa môže stať, že z času na čas vo vašom pripojení VPN zaznamenáte nejaký problém. Odstraňovanie problémov s vašou VPN nie je vždy jednoduchou úlohou. Musíte rozumieť svojmu systému a svojmu sieťovému prostrediu, ako aj komponentom, ktoré používate na ich správu. V nasledujúcich témach nájdete tipy na to, ako odstraňovať rozličné problémy, ktoré by ste mohli zaznamenať počas používania VPN:

Začíname s odstraňovaním problémov s VPN

V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Existuje niekoľko spôsobov, ako začať analýzu problémov s VPN:

1. Vždy sa presvedčte, či ste použili najnovšie dočasné opravy programu (PTF).
2. Skontrolujte, že to vyhovuje minimálnym požiadavkám pre nastavenie VPN.
3. Zobrazte všetky chybové správy, ktoré nájdete v okne Informácie o chybách alebo protokoloch úloh servera VPN pre lokálny aj vzdialený systém. V skutočnosti, keď riešite problémy s pripojením VPN, často je nevyhnutné prezrieť oba konce pripojenia. Okrem toho musíte vziať do úvahy, že je potrebné skontrolovať štyri adresy: Lokálne a vzdialené koncové body pripojenia, čo sú adresy, kde sa IPSec použije na pakety IP a lokálne a vzdialené koncové body údajov, čo sú zdrojové a cieľové adresy paketov IP.
4. Ak vami nájdené chybové správy neposkytujú dostatok informácií na vyriešenie problému, skontrolujte žurnál filtra IP.
5. Sledovanie komunikácie v systéme vám poskytuje ďalšie miesto, kde môžete nájsť všeobecné informácie o tom, či lokálny systém prijíma alebo odosiela požiadavky o pripojenie.
6. Príkaz Trace TCP Application (TRCTCPAPP) poskytuje ešte iný spôsob na izoláciu problémov. Príkaz TRCTCPAPP používa typicky Servis IBM na získanie výstupu sledovania z dôvodu analyzovania problémov s pripojením.

Súvisiace koncepty

“Požiadavky na nastavenie VPN” na strane 40
Aby pripojenie VPN fungovalo správne tak vo vašom systéme ako aj so sieťovými klientmi, musíte splniť minimálne tieto požiadavky.

“Odstraňovanie problémov s VPN pomocou protokolov úloh VPN” na strane 69
Keď sa pri vašom pripojení VPN stretnete s problémami, vždy je vhodné analyzovať protokoly úloh. V skutočnosti existuje niekoľko protokolov úloh, ktoré obsahujú chybové správy a iné informácie súvisiace s prostredím VPN.

“Odstraňovanie problémov s VPN so sledovaním komunikácií” na strane 74
IBM i5/OS poskytuje schopnosť na sledovanie údajov na komunikačnej linke, napríklad rozhraní LAN (Local Area Netowrk) alebo WAN (Wide Area Network). Priemerný užívateľ by nemusel porozumieť celému obsahu údajov o sledovaní. Ale položky sledovania môžete používať na zisťovanie, či sa uskutočnila výmena údajov medzi lokálnymi a vzdialenými systémami.

Súvisiace úlohy

“Zobrazovanie informácií o chybách” na strane 56
Táto úloha vám pomôže pri zisťovaní, prečo dochádza k chybe vo vašom pripojení.

“Odstraňovanie problémov s VPN pomocou žurnálu QIPFILTER” na strane 64
Tieto informácie zobrazte, ak sa chcete oboznámiť s filtrovacími pravidlami VPN.

“Spustenie pripojenia VPN” na strane 55
Pomocou tejto úlohy spustíte pripojenia, ktoré sa zahajujú lokálne.

Iné záležitosti na kontrolu

Ak sa vyskytne chyba po nastavení pripojenia a vy si nie ste istí, kde v sieti sa chyba vyskytla, skúste zjednodušiť vaše prostredie. Napríklad namiesto vyšetrovania častí pripojenia VPN naraz, začnite so samotným pripojením IP. Nasledovný zoznam uvádza niektoré základné smernice o tom, ako spustiť analýzu problémov s VPN, od najjednoduchšieho pripojenia IP až po zložité pripojenie VPN:

1. začnite s konfiguráciou IP medzi lokálnym a vzdialeným hostiteľom. Odstráňte všetky filtre IP na rozhraní, ktoré lokálny aj vzdialený systém používajú na komunikáciu. Funguje príkaz PING z lokálneho na vzdialeného hostiteľa?

   Poznámka: Oboznámte sa s výzvou pre príkaz PING; zadajte adresu vzdialeného systému, použite PF10 pre ďalšie parametre a potom zadajte lokálnu adresu IP. Toto je zvlášť dôležité, keď máte viaceré fyzické alebo logické rozhrania. Takto zaistíte, že sa do paketov PING umiestnia správne adresy.

   Ak odpoviete **áno**, prejdite ku kroku 2. Ak odpoviete **nie**, skontrolujte vašu konfiguráciu IP, stav rozhrania a položky smerovania. Ak je konfigurácia správna, na kontrolu napríklad toho, že požiadavka PING odišla zo systému, použite sledovanie komunikácie. Ak odošlete požiadavku PING ale nedostanete žiadnu odpoveď, problémom je najpravdepodobnejšie sieťový alebo vzdialený systém.

   Poznámka: Prenosy môžu prechádzať prechodovými smerovačmi alebo firewallmi, ktoré filtrujú IP pakety a môže filtrovať pakety PING. PING je väčšinou založený na protokole ICMP. Ak je PING úspešný, viete, že ste pripojený. Ak PING nie je úspešný, viete len to, že PING zlyhal. Možno by ste pri overovaní pripojenia medzi dvoma systémami mali vyskúšať iné protokoly IP, napríklad Telnet alebo FTP.
2. Skontrolujte pravidlá pre filtre pre VPN a presvedčte sa, či sú aktivované. Spustilo sa filtrovanie úspešne? Ak odpoviete **áno**, prejdite na krok 3. Ak odpoviete **nie**, skontrolujte existenciu chybových správ v okne Pravidlá pre pakety v System i Navigator. Uistite sa, že pravidlá pre filtre neurčujú Network Address Translation (NAT) pre žiadny prenos VPN.
3. Spustite vaše pripojenie VPN. Spustilo sa pripojenie úspešne? Ak odpoviete **áno**, prejdite ku kroku 4. Ak odpoviete **nie**, skontrolujte chyby v protokole úloh QTOVMAN a protokoloch úloh QTOKVPNIKE. Keď používate VPN, váš poskytovateľ internetových služieb (Internet Service Provider, ISP) a každá bezpečnostná brána vo vašej sieti musí podporovať protokoly Authentication Header (AH) a Encapsulated Security Payload (ESP). To, či zvolíte používať AH alebo ESP závisí na návrhoch, ktoré ste definovali pre vaše pripojenie VPN.
4. Ste schopní aktivovať reláciu užívateľa cez pripojenie VPN? Ak odpoviete **áno**, pripojenie VPN pracuje podľa očakávaní. Ak odpoviete **nie**, potom skontrolujte pravidlá pre pakety a skupiny dynamických kľúčov VPN a pripojenia pre definície filtrov, ktoré neumožňujú vami želaný užívateľský prenos.

Bežné chyby konfigurácie VPN a ako ich opravovať

Pomocou týchto informácií môžete získať prehľad o chybových hláseniach bežných chýb VPN a dozvedieť sa viac o možnostiach ich riešenia.

Poznámka: Počas konfigurácie VPN vytvárate niekoľko odlišných objektov konfigurácie, pričom každému z nich VPN požaduje aktivovať pripojenie. V termínoch GUI VPN, tieto objekty sú: Bezpečnostné politiky IP a Bezpečné pripojenia. Takže, keď tieto informácie odkazujú na objekt, odkazujú na jednu alebo viac týchto častí VPN.

Chybová správa VPN: TCP5B28

Keď sa pokúsite aktivovať pravidlá pre filtre na rozhranie, dostanete túto správu: TCP5B28 porušenie poradia CONNECTION_DEFINITION

Príznak:

Keď sa pokúsite aktivovať pravidlá pre filtre na špecifické rozhranie, dostanete túto chybovú správu:

```
TCP5B28: Porušenie poradia CONNECTION_DEFINITION
```

Možné riešenie:

Tieto pravidlá pre filtre, ktoré sa práve pokúšate aktivovať, obsahujú definície, ktoré boli usporiadané inak,

ako v predtým aktivovanej množine pravidiel. Najjednoduchším spôsobom, ako vyriešiť tento problém, je aktivovať súbor s pravidlami na **všetkých rozhraniach** namiesto na špecifickom rozhraní.

Chybová správa VPN: Položka sa nenašla

Keď kliknete pravým tlačidlom na objekt VPN a vyberiete **Vlastnosti** alebo **Vymazať**, dostanete správu, ktorá uvádza **Položka sa nenašla**.

Príznak:

Po kliknutí pravým tlačidlom myši na objekt v okne Budovanie VPN a výbere **Vlastnosti** alebo **Vymazať** sa zobrazí táto správa:

Možné riešenie:

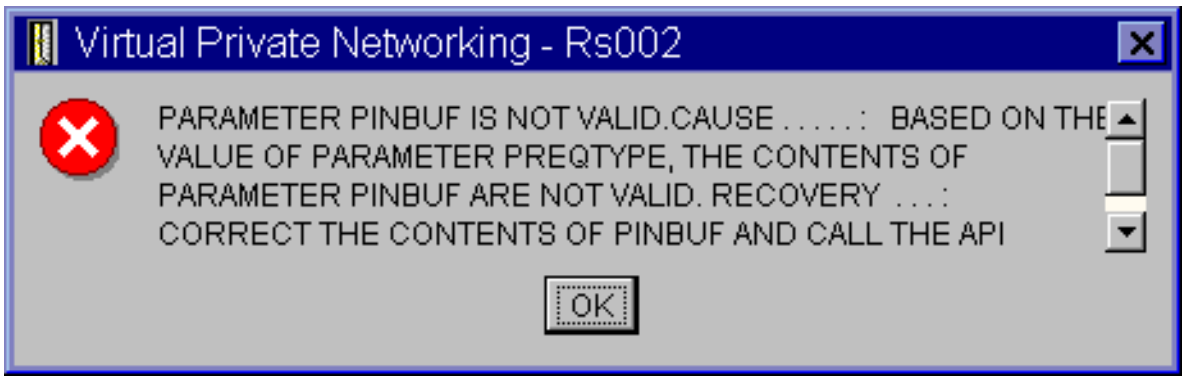
- Možno ste tento objekt vymazali, alebo ho premenovali a zatiaľ ste neaktualizovali okno. Následkom toho sa objekt stále zobrazuje v okne Virtuálne súkromné siete. Aby ste overili, či je to v tomto prípade tak, ponuky **Zobrazenie** vyberte **Obnoviť**. Ak sa objekt stále zobrazuje v okne Virtuálne súkromné siete, prejdite k ďalšej položke v tomto zozname.
- Keď ste konfigurovali vlastnosti tohto objektu, mohlo dôjsť k chybe v komunikácii medzi serverom VPN a vaším systémom. Veľa z objektov zobrazených v okne VPN sa vzťahuje na viac ako jeden objekt v databáze politík VPN. Chyba v komunikácii teda mohla spôsobiť, že niektoré z objektov v databáze sa naďalej vzťahujú na niektorý objekt vo VPN. Pri vytváraní alebo aktualizácii objektu vznikne chyba, ak nastane strata synchronizácie. Jediným spôsobom, ako tento problém opraviť, je vybrať **OK** v okne chyby. Spustí sa pracovný hárok vlastností pre chybný objekt. Len hárok vlastností bude obsahovať hodnotu. Všetko ostatné je prázdne (alebo obsahuje predvolené hodnoty). Zadajte správne atribúty objektu, vyberte **OK** a vaše zmeny sa uložia.
- Podobná chyba sa objaví, keď sa pokúsite vymazať objekt. Ak chcete opraviť tento problém, vyplňte prázdny hárok vlastností, ktorý sa otvorí, keď v chybovej správe kliknete na **OK**. Takto aktualizujete všetky odkazy na databázu politík VPN, ktoré boli stratené. Teraz môžete vymazať objekt.

Chybová správa VPN: PARAMETER PINBUF JE NEPLATNÝ

Pri pokuse o spustenie pripojenia ste získali správu s textom: **PARAMETER PINBUF NIE JE PLATNÝ...**

Príznak:

Pri pokuse o spustenie pripojenia ste získali správu, ktorá je podobná tomuto:



Možné riešenie:

To sa stane, keď váš systém je nastavený na používanie určitých umiestnení, na ktoré sa malé písmená správne nenamapovali. Ak chcete tento problém napraviť, skontrolujte, či všetky objekty používajú len veľké písmená alebo zmeňte umiestnenie systému.

Chybová správa VPN: Položka sa nenašla, Vzdialený server kľúčov...

Keď vyberiete **Vlastnosti** pre pripojenie dynamických kľúčov, dostanete chybu, ktorá uvádza, že server nemôže nájsť vzdialený server kľúčov, ktorý ste zadali.

Príznak:

Ak vyberiete **Vlastnosti** pre pripojenie dynamických kľúčov, zobrazí sa správa podobná tejto:

Možné riešenie:

Toto sa stane, keď vytvoríte pripojenie s príslušným vzdialeným serverom kľúčov a potom sa vzdialený server kľúčov odstráni zo svojej skupiny dynamických kľúčov. Na odstránenie problému kliknite v chybovej správe na **OK**. Otvorí sa hárok vlastností pre pripojenie dynamických kľúčov, ktoré sú chybné. Na tomto mieste môžete buď pridať vzdialený server kľúčov späť do skupiny dynamických kľúčov alebo vybrať iný identifikátor vzdialeného servera kľúčov. Kliknite na **OK**, aby sa vaše zmeny uložili.

Chybová správa VPN: Nedá sa aktualizovať objekt

Keď na pracovnom hárku vlastností pre skupinu dynamických kľúčov alebo manuálne pripojenie vyberiete **OK**, dostanete správu, ktorá vám oznámi, že systém nemôže aktualizovať objekt.

Príznak:

Ak na strane vlastností pre skupinu dynamických kľúčov alebo manuálneho pripojenia vyberiete **OK**, zobrazí sa táto správa:

.

Možné riešenie:

Táto chyba sa vyskytne, keď aktívne pripojenie práve používa objekt, ktorý sa pokúšate zmeniť. Na objekte v aktívnom pripojení nemôžete vykonávať zmeny. Ak chcete na objekte vykonať zmeny, identifikujte príslušné aktívne pripojenie, kliknite naň pravým tlačidlom a z následnej kontextovej ponuky vyberte **Zastaviť**.

Chybová správa VPN: Nedá sa zašifrovať kľúč...

Dostanete správu, ktorá oznámi, že systém nemôže zašifrovať vaše kľúče, lebo hodnota QRETSVRSEC musí byť nastavená na 1.

Príznak:

Zobrazí sa táto chybová správa:

Možné riešenie:

QRETSVRSEC je systémová hodnota, ktorá označuje, či váš systém môže v sebe ukladať zašifrované kľúče. Ak je táto hodnota nastavená na 0, dopredu zdieľané kľúče a kľúče pre algoritmy v manuálnom pripojení sa nemôžu ukladať do databázy politík VPN. Ak chcete tento problém napraviť, použite na váš systém reláciu emulácie 5250. Do príkazového riadku napíšte wrksysval a stlačte **Enter**. V zozname vyhľadajte QRETSVRSEC a vedľa toho napíšte 2 (zmeniť). Na ďalšom paneli napíšte 1 a stlačte **Enter**.

Súvisiace koncepty

"Chyba VPN: Všetky kľúče sú prázdne"
Keď zobrazíte vlastnosti manuálneho pripojenia, všetky dopredu zdieľané kľúče a kľúče algoritmu pre pripojenie sú prázdne.

Chybová správa VPN: CPF9821

Keď sa v System i Navigator pokúsite rozvinúť, alebo otvoriť kontajner Politiky IP, objaví sa správa CPF9821- Not authorized to program QTFRPRS in QSYS library.

Príznak:

Keď sa v System i Navigator pokúsite rozvinúť kontajner Politiky IP, objaví sa správa CPF9821- Not authorized to program QTFRPRS in QSYS library.

Možné riešenie:

Možno nemáte oprávnenie potrebné na získanie aktuálneho stavu Pravidiel paketov alebo správcu pripojení VPN. Ak chcete mať prístup k funkciám Pravidlá paketov v System i Navigator, overte si, či máte oprávnenie *IOSYSCFG.

Chyba VPN: Všetky kľúče sú prázdne

Keď zobrazíte vlastnosti manuálneho pripojenia, všetky dopredu zdieľané kľúče a kľúče algoritmu pre pripojenie sú prázdne.

Príznak:

Všetky dopredu zdieľané kľúče a kľúče algoritmov pre manuálne pripojenia sú prázdne.

Možné riešenie:

K tomuto dochádza pri každom nastavení systémovej hodnoty QRETSVRSEC na 0. Nastavením systémovej hodnoty na 0 sa vymažú všetky kľúče z databázy politík VPN. Ak chcete opraviť tento problém, musíte nastaviť systémovú hodnotu na 1 a potom znova zadať všetky kľúče. Pozrite si Chybovú správu: Nedajú sa zašifrovať kľúče, kde nájdete viac informácií o tom, ako to spraviť.

Súvisiace koncepty

"Chybová správa VPN: Nedá sa zašifrovať kľúč..."
Dostanete správu, ktorá oznámi, že systém nemôže zašifrovať vaše kľúče, lebo hodnota QRETSVRSEC musí byť nastavená na 1.

Chyba VPN: Pri používaní Pravidiel pre pakety sa objaví prihlásenie do iného systému

Ak prvýkrát použijete rozhranie Pravidiel pre pakety v System i Navigator, zobrazí sa prihlasovacia obrazovka do iného systému, ako je aktuálny.

Príznak:

Keď prvýkrát použijete pravidlá pre pakety, zobrazí sa prihlásenie do iného systému, ako je aktuálny.

Možné riešenie:

Pravidlá pre pakety na ukladanie bezpečnostných pravidiel pre pakety v integrovanom súborovom systéme používajú systém unicode. Dodatočné prihlásenie umožňuje System i Access for Windows získať príslušnú konverznú tabuľku pre Unicode. Toto nastane len jedenkrát.

Chyba VPN: Prázdny stav pripojenia v okne System i Navigator

Pripojenie nemá žiadnu hodnotu v stĺpci **Stav** v okne System i Navigator.

Príznak:

Pripojenie nemá žiadnu hodnotu v stĺpci **Stav** v okne System i Navigator.

Možné riešenie:

Prázdna hodnota stavu označuje, že pripojenie je v strede procesu spúšťania. Teda ešte nie je spustené, ale ani sa v ňom ešte nevyskytla chyba. Ak okno aktualizujete, pripojenie zobrazí stav Chyba, Povolené, Na požiadanie alebo Nečinné.

Chyba VPN: Pripojenie má po ukončení stav Povolené

Po zastavení pripojenia okno System i Navigator zobrazuje, že pripojenie je naďalej povolené.

Príznak:

Po zastavení pripojenia okno System i Navigator zobrazuje, že pripojenie je naďalej povolené.

Možné riešenie:

K tomuto typicky dochádza, ak ste ešte neobnovili okno System i Navigator. To znamená, že obsahuje neaktuálne informácie. Ak to chcete napraviť, z ponuky **Zobrazenie** vyberte **Obnoviť**.

Chyba VPN: 3DES nie je voľba pre šifrovanie

Keď pracujete s premenou politiky IKE, premenou údajovej politiky alebo manuálnym pripojením, šifrovací algoritmus 3DES nie je voľbou.

Príznak:

Keď pracujete s premenou politiky IKE, premenou údajovej politiky alebo manuálnym pripojením, šifrovací algoritmus 3DES nie je voľbou.

Možné riešenie:

S najväčšou pravdepodobnosťou je vo vašom systéme nainštalovaný len produkt Cryptographic Access Provider (5722-AC2) a nie produkt Cryptographic Access Provider (5722-AC3). Vzhľadom na obmedzenia dĺžok kľúčov poskytuje Cryptographic Access Provider (5722-AC2) len šifrovací algoritmus DES (Data Encryption Standard). Na povolenie šifrovania údajov v systémoch, v ktorých je spustený i5/OS V5R4 alebo novší, už nie je produkt Cryptographic Access Provider (5722-AC2) a (5722-AC3) potrebný.

Chyba VPN: Neočakávané stĺpce zobrazené v okne System i Navigator

Nastavíte stĺpce, ktoré chcete zobraziť v okne System i Navigator pre vaše pripojenia VPN a po ich neskoršom prezretí sa zobrazia odlišné stĺpce.

Príznak:

Nastavíte stĺpce, ktoré chcete zobraziť v okne System i Navigator pre vaše pripojenia VPN a po ich neskoršom prezretí sa zobrazia odlišné stĺpce.

Možné riešenie:

Keď zmeníte stĺpce na zobrazenie, zmeny nie sú špecifické pre konkrétneho užívateľa alebo PC, ale sú skôr celosystémové. Teda keď niekto iný zmení stĺpce v okne, zmeny postihnú každého, kto si na tomto systéme pozerá pripojenia.

Chyba VPN: Deaktivácia aktívnych pravidiel pre filtre zlyhala

Keď sa pokúsite deaktivovať aktuálnu množinu pravidiel pre filtre, v okne s výsledkami sa objaví správa Deaktivácia aktívnych pravidiel pre filtre zlyhala.

Príznak:

Keď sa pokúsite deaktivovať aktuálnu množinu pravidiel pre filtre, v okne s výsledkami sa objaví správa Deaktivácia aktívnych pravidiel pre filtre zlyhala.

Možné riešenie:

Väčšinou táto chybová správa znamená, že existuje minimálne jedno aktívne pripojenie VPN. Musíte zastaviť všetky pripojenia, ktoré majú stav povolené. Za týmto účelom kliknite pravým tlačidlom na aktívne pripojenia a vyberte **Zastaviť**. Teraz môžete deaktivovať filtrovacie pravidlá.

Chyba VPN: Skupina kľúčov pripojenia pre pripojenie sa zmenila

Keď vytvoríte pripojenie dynamických kľúčov, určíte skupinu dynamických kľúčov a identifikátor pre vzdialený server kľúčov. Neskôr, keď zobrazíte vlastnosti súvisiaceho objektu pripojenia, stránka Všeobecné v pracovnom hárku vlastnosti zobrazí rovnaký identifikátor vzdialeného servera kľúčov, ale inú skupinu dynamických kľúčov.

Príznak:

Keď vytvoríte pripojenie dynamických kľúčov, určíte skupinu dynamických kľúčov a identifikátor pre vzdialený server kľúčov. Neskôr, keď na súvisiacom objekte pripojenia vyberiete **Vlastnosti**, stránka **Všeobecné** na hárku vlastností zobrazí rovnaký identifikátor vzdialeného servera kľúčov, ale inú skupinu dynamických kľúčov.

Možné riešenie:

Identifikátor je jedinou informáciu uloženou v databáze politík VPN, ktorá odkazuje na vzdialený server kľúčov pripojenia dynamických kľúčov. Keď VPN hľadá politiku pre vzdialený server kľúčov, vyhľadá prvú skupinu dynamických kľúčov, ktorá má v sebe identifikátor vzdialeného servera kľúčov. Takže keď zobrazíte vlastnosti jedného z týchto pripojení, používa tú istú skupinu dynamických kľúčov, ktorú našla VPN. Ak nechcete priradiť skupinu dynamických kľúčov k tomuto vzdialenému serveru kľúčov, môžete vykonať jednu z nasledujúcich akcií:

1. Odstráňte vzdialený server kľúčov zo skupiny dynamických kľúčov.
2. V ľavej časti okna rozhrania VPN rozviňte **Podľa skupín** a presuňte želanú skupinu dynamických kľúčov do vrchnej časti tabuľky v pravej časti okna. Takto zabezpečíte, že VPN skontrolujte vzdialený server kľúčov v tejto skupine dynamických kľúčov, ako prvej.

Odstraňovanie problémov s VPN pomocou žurnálu QIPFILTER

Tieto informácie zobrazte, ak sa chcete oboznámiť s filtrovacími pravidlami VPN.

Žurnál IPFILTER sa nachádza v knižnici QUSRSYS a obsahuje informácie o množinách pravidiel pre filtre, ako aj informácie o tom, či bol datagram IP povolený alebo zakázaný. Protokolovanie sa vykonáva na základe voľby pre žurnálovanie, ktorú ste zadali vo svojich pravidlách pre filtre.

Súvisiace úlohy

"Začíname s odstraňovaním problémov s VPN" na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Povolenie žurnálu QIPFILTER

Editor Pravidiel pre pakety v System i Navigator použite na aktiváciu žurnálu QIPFILTER.

Protokolovaciu funkciu musíte povoliť pre každé filtrovacie pravidlo. Neexistuje žiadna funkcia, ktorá povoľuje protokolovanie pre všetky datagramy IP prichádzajúce na systém alebo odchádzajúce zo systému.

Poznámka: Ak chcete povoliť žurnál QIPFILTER, vaše filtre musia byť deaktivované.

Nasledujúce kroky popisujú, ako povoliť žurnálovanie pre konkrétne pravidlo pre filtre:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Konfigurácia**. Zobrazí sa rozhranie pre pravidlá pre pakety.
3. Otvorte existujúci súbor s pravidlami pre filtre.
4. Dvakrát kliknite na pravidlo pre filtre, ktoré chcete žurnálovať.
5. Na stránke **všeobecných nastavení** vyberte **ÚPLNÉ** v poli **Žurnálovanie** podľa vyššie uvedeného dialógového okna. Takto povolíte protokolovanie pre toto konkrétne pravidlo pre filtre.
6. Kliknite na **OK**.
7. Uložte a aktivujte zmenený súbor s pravidlami pre filtre.

Ak sa datagram IP zhoduje s pravidlom pre filtre, vytvorí sa položka v žurnáli QIPFILTER.

Používanie žurnálu QIPFILTER

i5/OS vytvorí žurnál automaticky pri prvej aktivácii filtrovania paketov IP.

Ak chcete v žurnáli zobraziť podrobnosti súvisiace s položkou, položky žurnálu môžete zobraziť na obrazovke alebo môžete použiť výstupný súbor. Skopírovaním položiek žurnálu do výstupného súboru môžete jednoducho zobraziť položky pomocou dotazovacích pomocných programov, ako je Query/400 alebo SQL. Môžete aj písať vlastné programy HLL na spracovanie položiek vo výstupnom súbore.

Nasleduje príklad príkazu Display Journal (DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Na skopírovanie položiek žurnálu QIPFILTER do výstupného súboru použite nasledujúce kroky:

1. Vytvorte kópiu systémom dodaného výstupného súboru QSYS/QATOFIPF do knižnice užívateľov pomocou príkazu Create Duplicate Object (CRTDUPOBJ). Nasleduje príklad príkazu CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(mojsubor)
   ```

2. Na skopírovanie položiek zo žurnálu QUSRSYS/QIPFILTER do výstupného súboru, ktorý ste vytvorili v predchádzajúcom kroku, použite príkaz Display Journal (DSPJRN).

Ak kopírujete DSPJRN do neexistujúceho výstupného súboru, systém súbor vytvorí, ale nebude obsahovať správne opisy polí.

Poznámka: Žurnál QIPFILTER obsahuje len položky povolenia a odmietnutia pre filtrovacie pravidlá, v ktorých je voľba žurnálovania nastavená na FULL. Napríklad, ak nastavíte iba filtrovacie pravidlá s hodnotou PERMIT, IP datagramy, ktoré nie sú explicitne povolené sú zakázané. Pre tieto zakázané datagramy sa do žurnálu nepridá žiadna položka. Za účelom analýzy problémov môžete pridať pravidlo pre filtre, ktoré výslovne zakáže všetok iný prenos a vykoná úplné žurnálovanie. Potom v žurnáli dostanete položky DENY pre všetky datagramy IP, ktoré sú zakázané. Kvôli výkonu sa neodporúča, aby ste povolili žurnálovanie pre všetky filtrovacie pravidlá. Keď sú vaše množiny filtrov otestované, obmedzte žurnálovanie na rozumnú podmnožinu položiek.

Súvisiace koncepty

"Žurnálové súbory QIPFILTER"
Pozrite si nasledujúcu tabuľku, ktorá popisuje polia vo výstupnom súbore QIPFILTER.

Žurnálové súbory QIPFILTER

Pozrite si nasledujúcu tabuľku, ktorá popisuje polia vo výstupnom súbore QIPFILTER.

Názov poľa	Dĺžka poľa	Numerické	Opis	Poznámka
TFENTL	5	Y	Dĺžka položky	
TFSEQN	10	Y	Sekvenčné číslo	

Názov poľa	Dĺžka poľa	Numerické	Opis	Poznámka
TFCODE	1	N	Žurnálový kód	Vždy M
TFENTT	2	N	Typ položky	Vždy TF
TFTIME	26	N	Časová značka SAA	
TFJOB	10	N	Názov úlohy	
TFUSER	10	N	Užívateľský profil	
TFNBR	6	Y	Číslo úlohy	
TFPGM	10	N	Názov programu	
TFRES1	51	N	Vyhradené	
TFUSPF	10	N	Užívateľ	
TFSYMN	8	N	Názov systému	
TFRES2	20	N	Vyhradené	
TFRESA	50	N	Vyhradené	
TFLINE	10	N	Popis linky	*ALL, ak TFREVT je U*, prázdne, ak TFREVT je L*, Názov linky, ak TFREVT je L
TFREVT	2	N	Udalosť pravidla	L* alebo L, keď sú pravidlá zavedené. U*, keď pravidlá sú nezavedené, A, pri akcii filtra
TFPDIR	1	N	Smer paketu IP	O je odchádzajúce, I je prichádzajúce
TFRNUM	5	N	Číslo pravidla	Aplikuje sa na číslo pravidla v súbore aktívnych súborov
TFACT	6	N	Vykonaná akcia filtra	PERMIT, DENY alebo IPSEC
TFPROT	4	N	Prenosový protokol	1 je ICMP 6 je TCP 17 je UDP 50 je ESP 51 je AH
TFSRCA	15	N	Adresa IP zdroja	
TFSRCP	5	N	Port zdroja	Odpad, ak TFPROT= 1 (ICMP)
TFDSTA	15	N	Adresa IP cieľa	
TFDSTP	5	N	Port cieľa	Odpad, ak TFPROT= 1 (ICMP)
TFTEXT	76	N	Doplnkový text	Obsahuje popis, ak TFREVT= L* alebo U*

Súvisiace úlohy

“Používanie žurnálu QIPFILTER” na strane 65
i5/OS vytvorí žurnál automaticky pri prvej aktivácii filtrovania paketov IP.

Odstraňovanie problémov s VPN pomocou žurnálu QVPN

Poskytuje informácie o premávke IP a pripojeniach.

Na protokolovanie informácií o prenose IP a pripojeniach používa VPN samostatný žurnál, nazývaný QVPN. QVPN je uložený v knižnici QUSRSYS. Kód žurnálu je M a typ žurnálu je TS. Položky žurnálu budete zriedkakedy používať každý deň. Skôr by pre vás mohli byť užitočné na odstraňovanie problémov a overovanie, či váš systém, kľúče a pripojenia fungujú vami určeným spôsobom. Položky žurnálu vám napríklad pomôžu porozumieť, čo sa deje s vašimi údajovými paketmi. Rovnako vás budú priebežne informovať o vašom aktuálnom stave VPN.

Povolenie žurnálu QVPN

Rozhranie Budovania VPN v System i Navigator použite na aktiváciu žurnálu VPN.

Neexistuje žiadna funkcia, ktorá povoľuje protokolovanie pre všetky pripojenia VPN. Preto musíte protokolovaciu funkciu povoliť pre každú skupinu dynamických kľúčov alebo manuálne pripojenie.

Nasledujúce kroky popisujú, ako povoliť funkciu žurnálovania pre konkrétnu skupinu dynamických kľúčov alebo manuálne pripojenie:

1. V System i Navigator rozviňte váš **systém → Network → IP Policies → Virtual Private Networking → Secure Connections**.
2. Pre skupinu dynamických kľúčov rozviňte **Podľa skupiny**, kliknite pravým tlačidlom na skupinu dynamických kľúčov, pre ktorú chcete povoliť žurnálovanie a vyberte **Vlastnosti**
3. Pre manuálne pripojenia rozviňte **Všetky pripojenia** a kliknite pravým tlačidlom na manuálne pripojenie, pre ktoré chcete povoliť žurnálovanie.
4. Na stránke **Všeobecné** vyberte žiadanú úroveň žurnálovania. Máte možnosť voľby zo štyroch volieb. Sú to tieto:

   Žiadna
   Pre túto skupinu pripojení sa nebude vykonávať žiadne žurnálovanie.

   Všetky Žurnálovanie sa bude vykonávať pre všetky činnosti pripojenia, ako je spúšťanie alebo zastavovanie pripojenia alebo obnovy kľúčov, ako aj informácie o prenose IP.

   Aktivita pripojenia
   Žurnálovanie sa bude vykonávať pre také činnosti pripojenia, ako je spúšťanie alebo zastavovanie pripojenia.

   Premávka IP
   Žurnálovanie sa bude vykonávať pre všetok prenos VPN, ktorý je spojený s týmto pripojením. Vždy, keď sa vyvolá pravidlo pre filtre, vytvorí sa položka protokolu. Systém zaznamenáva informácie o prenose IP v žurnáli QIPFILTER, ktorý sa nachádza v knižnici QUSRSYS.
5. Kliknite na **OK**.
6. Spustite pripojenie na aktiváciu žurnálovania.

Poznámka: Pred zastavením žurnálovania skontrolujte, že pripojenie je neaktívne. Ak chcete zmeniť stav skupiny pripojení, uistite sa, že s touto konkrétnou skupinou nie sú spojené žiadne aktívne pripojenia.

Používanie žurnálu QVPN

Ak chcete v žurnáli VPN zobraziť podrobnosti súvisiace s položkou, položky môžete zobraziť na obrazovke alebo môžete použiť výstupný súbor.

Skopírovaním položiek žurnálu do výstupného súboru môžete jednoducho zobraziť položky pomocou dotazovacích pomocných programov, ako je Query/400 alebo SQL. Môžete aj písať vlastné programy HLL na spracovanie položiek vo výstupnom súbore. Nasleduje príklad príkazu Display Journal (DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mojakniznica/mojsubor) ENTDTALEN(*VARLEN *CALC)
```

Na skopírovanie položiek žurnálu VPN do výstupného súboru použite nasledujúce kroky:

.

1. Vytvorte kópiu systémom dodaného výstupného súboru QSYS/QATOVSOF do knižnice užívateľov. To môžete vykonať pomocou príkazu Create Duplicate Object (CRTDUPOBJ). Nasleduje príklad príkazu CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
       NEWOBJ(mojsubor)
   ```

2. Na skopírovanie položiek zo žurnálu QUSRSYS/QVPN do výstupného súboru vytvoreného v predchádzajúcom kroku, použite príkaz Display Journal (DSPJRN). Ak sa pokúšate kopírovať DSPJRN do neexistujúceho výstupného súboru, systém súbor vytvorí, ale nebude obsahovať správne opisy polí.

Súvisiace koncepty

"Žurnálové súbory QVPN"
Pozrite si nasledujúcu tabuľku, ktorá popisuje polia vo výstupnom súbore QVPN.

Žurnálové súbory QVPN

Pozrite si nasledujúcu tabuľku, ktorá popisuje polia vo výstupnom súbore QVPN.

Názov poľa	Dĺžka poľa	Numerické	Opis	Poznámka
TSENTL	5	Y	Dĺžka položky	
TSSEQN	10	Y	Sekvenčné číslo	
TSCODE	1	N	Žurnálový kód	Vždy M
TSENTT	2	N	Typ položky	Vždy TS
TSTIME	26	N	Časová značka položky SAA	
TSJOB	10	N	Názov úlohy	
TSUSER	10	N	Užívateľ úlohy	
TSNBR	6	Y	Číslo úlohy	
TSPGM	10	N	Názov programu	
TSRES1	51	N	Nepoužíva sa	
TSUSPF	10	N	Názov užívateľského profilu	
TSSYNM	8	N	Názov systému	
TSRES2	20	N	Nepoužíva sa	
TSRESA	50	N	Nepoužíva sa	
TSESDL	4	Y	Dĺžka špecifických údajov	
TSCMPN	10	N	Komponent VPN	
TSCONM	40	N	Názov pripojenia	
TSCOTY	10	N	Typ pripojenia	
TSCOS	10	N	Stav pripojenia	
TSCOSD	8	N	Dátum spustenia	
TSCOST	6	N	Čas spustenia	
TSCOED	8	N	Dátum ukončenia	
TSCOET	6	N	Čas ukončenia	
TSTRPR	10	N	Prenosový protokol	
TSLCAD	43	N	Adresa lokálneho klienta	
TSLCPR	11	N	Lokálne porty	

Názov poľa	Dĺžka poľa	Numerické	Opis	Poznámka
TSRCAD	43	N	Adresa vzdialeného klienta	
TSCPR	11	N	Vzdialené porty	
TSLEP	43	N	Lokálny koncový bod	
TSREP	43	N	Vzdialený koncový bod	
TSCORF	6	N	Počet obnovení	
TSRFDA	8	N	Dátum najbližšieho obnovenia	
TSRFTI	6	N	Čas najbližšieho obnovenia	
TSRFLS	8	N	Životná veľkosť obnovenia	
TSSAPH	1	N	Fáza SA	
TSAUTH	10	N	Typ autentifikácie	
TSENCR	10	N	Typ šifrovania	
TSDHGR	2	N	Skupina Diffie-Hellmana	
TSERRC	8	N	Chybový kód	

Súvisiace úlohy

“Používanie žurnálu QVPN” na strane 67
Ak chcete v žurnáli VPN zobraziť podrobnosti súvisiace s položkou, položky môžete zobraziť na obrazovke alebo môžete použiť výstupný súbor.

Odstraňovanie problémov s VPN pomocou protokolov úloh VPN

Keď sa pri vašom pripojení VPN stretnete s problémami, vždy je vhodné analyzovať protokoly úloh. V skutočnosti existuje niekoľko protokolov úloh, ktoré obsahujú chybové správy a iné informácie súvisiace s prostredím VPN.

Ak oboma stranami pripojenia sú modely System i, je dôležité, aby ste analyzovali protokoly úloh na oboch stranách tohto pripojenia. Keď spustenie dynamického pripojenia zlyhá, je užitočné, ak porozumiete tomu, čo sa deje na vzdialenom systéme.

Úlohy VPN, QTOVMAN a QTOKVPNIKE, pracujú v subsystéme QSYSWRK. Príslušné protokoly úloh môžete zobraziť z System i Navigator.

Táto časť predstavuje najdôležitejšie úlohy pre prostredie VPN. Nasledujúci zoznam zobrazuje názvy úloh so stručným vysvetlením, na čo sa ktorá úloha používa:

QTCPIP
Táto úloha je základná úloha, ktorá spúšťa všetky rozhrania TCP/IP. Ak máte všeobecne zásadné problémy s TCP/IP, analyzujte protokol úloh QTCPIP.

QTOKVPNIKE
Úloha QTOKVPNIKE je úloha správcu kľúčov VPN. Správca kľúčov VPN načúva na UDP porte 500, aby vykonával spracovanie protokolu Internet Key Exchange (IKE).

QTOVMAN
Táto úloha je správca pripojení pre pripojenia VPN. Príslušný protokol úloh obsahuje správy pre každý pokus o pripojenie, ktorý zlyhá.

QTPPANSxxx

Táto úloha sa používa pre telefonické pripojenia PPP. Odpovedá na pokusy o pripojenie, kde *ANS je definované v profile PPP.

QTPPPCTL

Toto je úloha PPP pre výstupné telefonické pripojenia.

QTPPPL2TP

Toto je úloha správcu protokolu Layer Two Tunneling Protocol (L2TP). Ak máte problémy s nastavovaním tunela L2TP, pozrite si správy v tomto protokole úloh.

Súvisiace úlohy

"Začíname s odstraňovaním problémov s VPN" na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Chybové správy Správcu pripojení VPN

Ak pri pripojení VPN dôjde k nejakej chybe, zaprotokoluje Správca pripojenia VPN v protokole úlohy QTOVMAN dve správy.

Prvá správa poskytuje podrobnosti ohľadne chyby. Informácie o týchto chybách si môžete pozrieť v System i Navigator kliknutím pravým tlačidlom myši na pripojenie s chybou a výberom **Informácie o chybe**.

Druhá správa popisuje akciu, ktorú ste sa pokúšali na pripojení vykonať, keď sa vyskytla chyba. Napríklad jeho spustenie alebo zastavenie. Správy TCP8601, TCP8602 a TCP860A sú typickými príkladmi druhých správ.

Chybové správy Správcu pripojení VPN

Správa	Príčina	Zotavenie
TCP8601 Nebolo možné spustiť pripojenie VPN [*názov pripojenia*]	Nebolo možné spustiť toto pripojenie VPN kvôli jednému z týchto kódov príčin: *0* - Predošlá správa v protokole úloh s rovnakým názvom pripojenia VPN má detailnejšie informácie. *1* - Konfigurácia politiky VPN. *2* - Zlyhanie sieťovej komunikácie. *3* - Správca kľúčov VPN zlyhal pri vyjednávaní novej bezpečnostnej asociácie. *4* - Vzdialený koncový bod pre toto pripojenie nie je správne nakonfigurovaný. *5* - Správca kľúčov VPN zlyhal pri odpovedaní Správcovi pripojení VPN. *6* - Zlyhanie zavedenia pripojenia VPN bezpečnostného komponentu IP. *7* - Zlyhanie komponentu PPP.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Opravte chyby a skúste požiadavku znova. 3. Použite System i Navigator, aby ste zobrazili stav pripojenia. Pripojenia, ktoré sa nedali spustiť, budú v chybovom stave.
TCP8602 Došlo k chybe pri zastavení pripojenia VPN [*názov pripojenia*]	Zadané pripojenie VPN síce prijalo požiadavku o zastavení, ale nezastavilo sa kvôli jednému z týchto kódov príčin: *0* - Predošlá správa v protokole úloh s rovnakým názvom pripojenia VPN má detailnejšie informácie. *1* - Pripojenie VPN neexistuje. *2* - Zlyhanie internej komunikácie so Správcom kľúčov VPN. *3* - Zlyhanie internej komunikácie s komponentom IPSec. *4* - Zlyhanie komunikácie so vzdialeným koncovým bodom pripojenia VPN.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Opravte chyby a skúste požiadavku znova. 3. Použite System i Navigator, aby ste zobrazili stav pripojenia. Pripojenia, ktoré sa nedali spustiť, budú v chybovom stave.

Chybové správy Správcu pripojení VPN

Správa	Príčina	Zotavenie
TCP8604 Zlyhalo spustenie pripojenia VPN [*názov pripojenia*]	Spustenie tohto pripojenia VPN zlyhalo kvôli jednému z týchto kódov príčin: *1* - Nebolo možné preložiť názov vzdialeného hostiteľa na adresu IP. *2* - Nedal sa preložiť názov lokálneho hostiteľa na adresu IP. *3* - Pravidlo pre filter politiky VPN spojené s týmto pripojením VPN nie je zavedené. *4* - Užívateľom zadaná hodnota kľúča nie je platná pre tento priradený algoritmus. *5* - Inicializačná hodnota pre pripojenie VP nepovoľuje zadanú akciu. *6* - Rola systému pre pripojenie VPN je nekonzistentná s informáciami zo skupiny pripojení. *7* - Vyhradené. *8* - Koncové body údajov (lokálne a vzdialené adresy a služby) tohto pripojenia VPN sú nekonzistentné s informáciami zo skupiny pripojení. *9* - Typ identifikátora je neplatný.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Opravte chyby a skúste požiadavku znova. 3. Použite System i Navigator, aby ste skontrolovali alebo opravili konfiguráciu politiky VPN. Skontrolujte, či skupina dynamických kľúčov priradené k tomuto pripojeniu má nakonfigurované prijateľné hodnoty.
TCP8605 Správca pripojení VPN nemohol komunikovať so Správcom kľúčov VPN	Správca pripojení VPN vyžaduje, aby služby Správcu kľúčov VPN vytvorili bezpečnostné asociácie pre dynamické pripojenia VPN. Správca pripojení VPN nemohol komunikovať so Správcom kľúčov VPN.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Pomocou príkazu NETSTAT OPTION(*IFC) overte, či rozhranie *LOOPBACK je aktívne. 3. Pomocou príkazu ENDTCPSVR SERVER(*VPN) ukončite server VPN. Potom pomocou príkazu STRTCPSRV SERVER(*VPN) reštartujte server VPN. **Poznámka:** Toto má za následok ukončenie všetkých aktuálnych pripojení VPN.
TCP8606 Správca kľúčov VPN nemohol vytvoriť požadované bezpečnostné priradenie pre pripojenie [*názov pripojenia*]	Správca kľúčov VPN nemohol vytvoriť požadované bezpečnostné priradenie kvôli jednému z týchto kódov príčin: *24* - Zlyhala autentifikácia pripojenia kľúča Správcu kľúčov VPN. *8300* - Vyskytlo sa zlyhanie počas vyjednávania pripojenia kľúča Správcu kľúčov VPN. *8306* - Nenašiel sa žiadny lokálny dopredu zdieľaný kľúč. *8307* - Nenašla sa žiadna politika fázy 1 vzdialenej IKE. *8308* - Nenašiel sa žiadny vzdialený dopredu zdieľaný kľúč. *8327* - Časový limit vyjednávania pripojenia kľúča Správcu kľúčov VPN uplynul. *8400* - Vyskytlo sa zlyhanie počas vyjednávania pripojenia VPN Správcu kľúčov VPN. *8407* - Nenašla sa žiadna politika fázy 2 vzdialenej IKE. *8408* - Časový limit vyjednávania pripojenia VPN Správcu kľúčov VPN uplynul. *8500 or 8509* - Vyskytla sa chyba siete Správcu kľúčov VPN.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Opravte chyby a skúste požiadavku znova. 3. Použite System i Navigator, aby ste skontrolovali alebo opravili konfiguráciu politiky VPN. Skontrolujte, či skupina dynamických kľúčov priradené k tomuto pripojeniu má nakonfigurované prijateľné hodnoty.

Chybové správy Správcu pripojení VPN

Správa	Príčina	Zotavenie
TCP8608 Pripojenie VPN [*názov pripojenia*] nemohlo získať adresu NAT	Táto skupina dynamických kľúčov alebo pripojenie údajov špecifikovalo, že NAT (Network Address Translation) sa bude vykonávať na jednej alebo viacerých adresách a že pravdepodobne zlyhalo kvôli jednému z týchto kódov príčin: *1* - Adresa pre použitie s NAT nie je samostatná adresa IP. *2* - Všetky dostupné adresy sa už použili.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ. 2. Opravte chyby a skúste požiadavku znova. 3. Použite System i Navigator, aby ste skontrolovali alebo opravili politiku VPN. Skontrolujte, či skupina dynamických kľúčov priradené k tomuto pripojeniu má nakonfigurované prijateľné hodnoty pre adresy.
TCP8620 Koncový bod lokálneho pripojenia je nedostupný	Tieto pripojenia VPN sa nedali povoliť, lebo koncový bod lokálneho pripojenia nebol k dispozícii.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Pomocou príkazu NETSTAT OPTION(*IFC) skontrolujte, či koncový bod lokálneho pripojenia je definovaný a spustený. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8621 Koncový bod lokálnych údajov je nedostupný	Toto pripojenie VPN sa nedalo povoliť, lebo koncový bod lokálnych údajov nebol k dispozícii.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Pomocou príkazu NETSTAT OPTION(*IFC) skontrolujte, či koncový bod lokálneho pripojenia je definovaný a spustený. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8622 Zapuzdrenie prenosu nie je povolené s bránou	Toto pripojenie VPN sa nedalo povoliť, lebo dohodnutá politika určila režim zapuzdrenia prenosu a toto pripojenie je definované ako bezpečnostná brána.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zmenili politiku VPN priradenú k tomuto pripojeniu VPN. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8623 Pripojenie VPN sa prekrýva s existujúcim pripojením	Toto pripojenie VPN sa nedalo povoliť, lebo existujúce pripojenie VPN je už povolené. Toto pripojenie má lokálny koncový bod [*hodnota lokálneho koncového bodu*] a vzdialený koncový bod [*hodnota vzdialeného koncového bodu*].	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zobrazili všetky povolené pripojenia, ktorých koncové body lokálnych a vzdialených údajov prekrývajú dané pripojenie. Ak sa vyžadujú oba pripojenia, zmeňte politiku existujúceho pripojenia. 3. Opravte všetky chyby a skúste požiadavku znova.

Chybové správy Správcu pripojení VPN

Správa	Príčina	Zotavenie
TCP8624 Pripojenie VPN je nad rámec priradeného pravidla pre filtre politiky	Toto pripojenie VPN sa nedalo povoliť, lebo koncové body údajov nie sú v rozsahu definovaného pravidla pre filtre politiky.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zobrazili obmedzenia koncového bodu údajov pre toto pripojenie alebo skupinu dynamických kľúčov. Ak je vybrané **Podmnožina filtrov politiky** alebo **Prispôsobiť na zhodu filtra politiky**, skontrolujte koncové body údajov pripojenia. Tieto musia vyhovovať aktívnemu pravidlu pre filtre, ktoré má k tomuto pripojeniu priradenú akciu IPSEC a názov pripojenia VPN. Ak chcete povoliť toto pripojenie, zmeňte politiku existujúceho pripojenia alebo pravidla pre filtre. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8625 Pripojenie VPN neprešlo cez kontrolu algoritmom ESP	Toto pripojenie VPN sa nedalo povoliť, lebo tajný kľúč priradený k pripojeniu bol nedostatočný.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zobrazili politiku priradenú k tomuto pripojeniu a vložili odlišný tajný kľúč. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8626 Koncový bod pripojenia VPN nie je rovnaký ako koncový bod údajov	Toto pripojenie VPN sa nedalo povoliť, lebo politika určuje, že je to hostiteľ a koncový bod pripojenia VPN nie je rovnaký ako koncový bod údajov.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zobrazili obmedzenia koncového bodu údajov pre toto pripojenie alebo skupinu dynamických kľúčov. Ak je vybrané **Podmnožina filtrov politiky** alebo **Prispôsobiť na zhodu filtra politiky**, skontrolujte koncové body údajov pripojenia. Tieto musia vyhovovať aktívnemu pravidlu pre filtre, ktoré má k tomuto pripojeniu priradenú akciu IPSEC a názov pripojenia VPN. Ak chcete povoliť toto pripojenie, zmeňte politiku existujúceho pripojenia alebo pravidla pre filtre. 3. Opravte všetky chyby a skúste požiadavku znova.

Chybové správy Správcu pripojení VPN

Správa	Príčina	Zotavenie
TCP8628 Pravidlo pre filtre politiky nebolo zavedené	Pravidlo pre filtre politiky pre toto pripojenie nie je aktívne.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zobrazili aktívne filtre politiky. Skontrolujte pravidlo pre filtre politiky pre toto pripojenie. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8629 Paket IP bol zrušený pre pripojenie VPN	Toto pripojenie VPN má nakonfigurované VPN NAT a vyžadovaná množina adries NAT prekročila dostupné adresy NAT.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Použite System i Navigator, aby ste zvýšili počet adries NAT priradených k tomuto pripojeniu VPN. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP862A Zlyhalo spustenie pripojenia PPP	Toto pripojenie VPN bolo priradené k profilu PPP. Keď bolo spustené, vykonal sa pokus o spustenie profilu PPP, ale nastalo zlyhanie.	1. Skontrolujte protokoly úloh, kde nájdete možno viac správ prislúchajúcich tomuto pripojeniu. 2. Skontrolujte protokol úloh priradený k tomuto pripojeniu PPP. 3. Opravte všetky chyby a skúste požiadavku znova.

Súvisiace úlohy

“Zobrazenie atribútov aktívnych pripojení” na strane 56
Vykonajte túto úlohu na kontrolu stavu a iných atribútov vašich aktívnych pripojení.

Odstraňovanie problémov s VPN so sledovaním komunikácií

IBM i5/OS poskytuje schopnosť na sledovanie údajov na komunikačnej linke, napríklad rozhraní LAN (Local Area Netowrk) alebo WAN (Wide Area Network). Priemerný užívateľ by nemusel porozumieť celému obsahu údajov o sledovaní. Ale položky sledovania môžete používať na zisťovanie, či sa uskutočnila výmena údajov medzi lokálnymi a vzdialenými systémami.

Spustenie sledovania komunikácie

Na spustenie sledovania komunikácie na vašom systéme použite príkaz Start Communications Trace (STRCMNTRC). Nasleduje príklad príkazu STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('Problémy s VPN')
```

Parametre príkazu sú vysvetlené v nasledujúcom zozname:

CFGOBJ (objekt konfigurácie)
Názov objektu konfigurácie na sledovanie. Objekt je buď popis linky, popis sieťového rozhrania alebo popis sieťového servera.

CFGTYPE (typ konfigurácie)
Či sa sleduje linka (*LIN), sieťové rozhranie (*NWI) alebo sieťový server (*NWS).

MAXSTG (veľkosť pamäťového bloku)
Veľkosť vyrovnávacej pamäte pre sledovanie. Predvolená hodnota je 128 KB. Rozsah je 128 KB až 64 MB.

Aktuálna celosystémová maximálna veľkosť vyrovnávacej pamäte sa definuje v System Service Tools (SST). Preto sa môže stať, že ak v príkaze STRCMNTRC použijete väčšiu veľkosti vyrovnávacej pamäte, než je veľkosť zadefinovaná v SST, môžete byť zobrazené chybové hlásenie. Nezabudnite, že suma veľkostí vyrovnávacej pamäte na všetkých spustených komunikačných sledovaniach nesmie prekročiť maximálnu veľkosť vyrovnávacej pamäte definovanej v SST.

DTADIR (smer prenosu údajov)
Smer prenosu údajov na sledovanie. Smer môže byť len odchádzajúci prenos (*SND), len prichádzajúci prenos (*RCV, alebo oba smery (*BOTH).

TRCFULL (sledovanie plné)
Čo sa stane, keď je vyrovnávacia pamäť sledovania plná. Tento parameter má dve prípustné hodnoty. Predvolená hodnota je *WRAP, čo znamená, že keď je vyrovnávacia pamäť sledovania plná, nastane návrat na jej začiatok. V tomto prípade sa začnú prepisovať najstaršie záznamy novými záznamami.

Druhá hodnota *STOPTRC zastaví sledovanie, keď je vyrovnávacia pamäť, zadaná v parametri MAXSTG, plná záznamov o sledovaní. Všeobecne platí, vždy definujte vyrovnávaciu pamäť dostatočne veľkú na uloženie všetkých záznamov o sledovaní. Ak dôjde k zacykleniu sledovania, môžete prísť o dôležité informácie sledovania. Ak narazíte na tento veľmi zriedkavý problém, definujte vyrovnávaciu pamäť dostatočne veľkú, aby návrat na začiatok vyrovnávacej pamäte nevymazal žiadne dôležité informácie.

USRDTA (počet užívateľských bajtov na sledovanie)
Definuje množstvo údajov, ktoré sa majú sledovať v časti užívateľských údajov v údajových rámcoch. Štandardne sa pre rozhrania LAN zachytáva len prvých 100 bajtov užívateľských údajov. Pre všetky ostatné rozhrania sa zachytávajú všetky užívateľské údaje. Uistite sa, že ste zadali *MAX, ak sa obávate problémov v užívateľských údajoch rámca.

TEXT (opis sledovania)
Poskytuje účelný popis sledovania.

Zastavenie sledovania komunikácie

Ak nezadáte inak, sledovanie zvyčajne zastaví ihneď po nastaní podmienok, na ktoré je sledovanie nastavené. Na zastavenie sledovania použite príkaz End Communications Trace (ENDCMNTRC). Nasledujúci príkaz je príkladom príkazu ENDCMNTRC:

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

Príkaz má dva parametre:

CFGOBJ (objekt konfigurácie)
Názov objektu konfigurácie, na ktorom prebieha sledovanie. Objekt je buď popis linky, popis sieťového rozhrania alebo popis sieťového servera.

CFGTYPE (typ konfigurácie)
Či sa sleduje linka (*LIN), sieťové rozhranie (*NWI) alebo sieťový server (*NWS).

Tlač údajov sledovania

Keď zastavíte sledovanie komunikácie, budete potrebovať vytlačiť sledované údaje. Na vykonanie tejto úlohy použite príkaz Print Communications Trace (PRTCMNTRC). Keďže všetok prenos na linke sa počas doby sledovania zachytáva, máte na generovanie výstupu viacero volieb pre filtre. Skúste udržať spoolový súbor podľa možností čo najmenší. Takto bude analýza rýchlejšia a účinnejšia. V prípade problémov s VPN, filtrujte len na IP prenose a ak je to možné, na špecifickej IP adrese. Tiež máte voľbu filtrovať na špecifickom čísle portu IP. Nasleduje príklad príkazu PRTCMNTRC:

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

V tomto príklade sa sledovanie formátuje pre prenos IP a obsahuje len údaje pre adresu IP, kre zdrojová alebo cieľová adresa je 10.50.21.1 a zdrojové alebo cieľové číslo IP je 500.

Nasleduje výklad len najdôležitejších parametrov príkazov na analýzu problémov s VPN:

CFGOBJ (objekt konfigurácie)
Názov objektu konfigurácie, na ktorom prebieha sledovanie. Objekt je buď popis linky, popis sieťového rozhrania alebo popis sieťového servera.

CFGTYPE (typ konfigurácie)
Či sa sleduje linka (*LIN), sieťové rozhranie (*NWI) alebo sieťový server (*NWS).

FMTTCP (formátovať údaje TCP/IP)
Či formátovať sledovanie pre údaje TCP/IP a UDP/IP. Zadajte *YES, ak chcete formátovať sledovanie údajov IP.

TCPIPADR (formátovať údaje TCP/IP podľa adresy)
Tento parameter pozostáva z dvoch prvkov. Ak zadáte adresy IP na oboch prvkoch, vytlačí sa prenos IP len medzi týmito dvoma adresami.

SLTPORT (číslo portu IP)
Číslo portu IP na filtrovanie.

FMTBCD (formátovať údaje broadcast)
Či sa budú tlačiť všetky vysielané rámiky. Predvolená hodnota je Áno. Ak nechcete zobrazovať napríklad požiadavky ARP (Address Resolution Protocol), zadajte *NO; v opačnom prípade môžete byť zahltený prijatými správami.

Súvisiace úlohy

“Začíname s odstraňovaním problémov s VPN” na strane 58
V tejto úlohe sa oboznámte s rozličnými metódami rozpoznávania problémov s VPN, ktoré zaznamenáte vo vašom systéme.

Súvisiace informácie pre VPN

Nasledujúce publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia so súhrnom tém Virtuálne súkromné siete. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

IBM Redbooks

- IBM System i Security Guide for IBM i5/OS verzia 5 vydanie 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

Webové stránky

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

Príloha. Poznámky

Tieto informácie boli vyvinuté pre produkty a služby poskytované v USA.

IBM nemusí produkty, služby alebo komponenty, o ktorých sa hovorí v tomto dokumente, ponúkať v iných krajinách. Informácie o produktoch a službách, aktuálne dostupných vo vašej krajine, môžete získať od zástupcu spoločnosti IBM. Akékoľvek odkazy na produkt, program alebo službu IBM nemajú byť chápané ako výslovná či mlčky predpokladaná povinnosť použiť jedine tento produkt, program alebo službu. Môžete použiť ľubovoľný funkčne ekvivalentný produkt, program alebo službu, ktoré neporušujú práva duševného vlastníctva IBM. Užívateľ však zodpovedá za to, aby zhodnotil a overil používanie takéhoto produktu, programu alebo služby.

IBM môže vlastniť patenty alebo mať podané žiadosti o patenty, týkajúce sa predmetnej veci popísanej v tomto dokumente. Získanie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Informácie o licenciách získate u výrobcu na adrese:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Informácie o licenciách týkajúcich sa DBCS získate vo vašej krajine od IBM Intellectual Property Department alebo na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Nasledujúci odsek sa netýka Veľkej Británie alebo akejkoľvek inej krajiny, v ktorej sú takéto ustanovenia nezlučiteľné s miestnym zákonom: INTERNATIONAL BUSINESS MACHINES CORPORATION POSKYTUJE TÚTO PUBLIKÁCIU “TAK AKO JE” BEZ AKÝCHKOĽVEK GARANCIÍ, ČI UŽ VYJADRENÝCH ALEBO IMPLIKOVANÝCH, ALE NEOBMEDZENÝCH NA IMPLIKOVANÉ GARANCIE NEPORUŠENIA, SCHOPNOSTI UVEDENIA NA TRH ALEBO SPÔSOBILOSTI NA URČITÝ ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných ani mlčky predpokladaných záruk v určitých operáciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

Tento dokument môže obsahovať technické nepresnosti alebo tlačové chyby. Informácie uvedené v tomto dokumente podliehajú priebežným zmenám; tieto zmeny budú zapracované do nových vydaní. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných v tejto publikácii.

Akékoľvek odkazy v tejto publikácii na iné webové stránky, než stránky firmy IBM, sú poskytované len pre vaše pohodlie a v žiadnom prípade neslúžia ako súhlas s týmito webovými stránkami. Materiály, uvedené na týchto webových stránkach, nie sú súčasťou materiálov tohto produktu IBM a ich použitie je na vaše vlastné riziko.

IBM môže použiť alebo distribuovať ľubovoľné vami poskytnuté informácie vhodným zvoleným spôsobom bez toho, aby tým voči vám vznikli akékoľvek záväzky.

Držitelia licencií tohto programu, ktorí si želajú mať informácie o tomto programe kvôli povoleniu: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) spoločného používania vymenených informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť v niektorých prípadoch dostupné až po zaplatení príslušného poplatku.

Licenčný program, ktorý je popísaný v tomto dokumente a vo všetkých k nemu dostupných licenčných materiáloch, je spoločnosťou IBM poskytovaný za podmienok uvedených v zmluvách IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code alebo v akejkoľvek rovnocennej medzi nami uzatvorenej zmluve.

Akékoľvek tu uvedené údaje o výkone, boli určené v regulovanom prostredí. Preto sa môžu výsledky získané v iných prevádzkových prostrediach výrazne odlišovať. Niektoré merania boli vykonané vo vývojovom systéme a preto nie je žiadna záruka, budú tieto merania rovnaké aj na všeobecne dostupných systémoch. Navyše, niektoré merania mohli byť vykonané extrapoláciou. Aktuálne výsledky sa môžu rôzniť. Užívatelia týchto dokumentov by si mali overiť príslušné údaje pre svoje konkrétne prostredie.

Informácie týkajúce sa produktov iných spoločností ako IBM boli získané od dodávateľov týchto produktov, z ich publikovaných oznámení alebo iných verejne prístupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani iné parametre týkajúce sa produktov nepochádzajúcich od IBM. Otázky o schopnostiach produktov nepochádzajúcich od IBM adresujte dodávateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúcich zámerov IBM sa môžu zmeniť alebo zrušiť bez predchádzajúceho upozornenia a majú len informatívny charakter.

Tieto informácie obsahujú príklady údajov a hlásení z každodenných pracovných operácií. Kvôli čo najlepšej pochopiteľnosti obsahujú aj konkrétne mená osôb, názvy spoločností a produktov. Všetky tieto mená a názvy sú vymyslené a akákoľvek podobnosť so skutočnými menami, názvami a adresami je čisto náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete akoukoľvek formou kopírovať, modifikovať a distribuovať bez poplatkov pre IBM s cieľom vývoja, používania, marketingu alebo distribúcie aplikačných programov vyhovujúcim rozhraniu aplikačných programov pre operačnú platformu, pre ktoré sú vzorové programy napísané. Tieto príklady neboli dôkladne testované na všetky podmienky. Z tohto dôvodu spoločnosť IBM nemôže zaručiť alebo predpokladať spoľahlivosť, prevádzkyschopnosť alebo funkciu týchto programov.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov spoločnosti IBM. © Copyright IBM Corp. _uveďte rok alebo roky_. Všetky práva vyhradené.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Informácie o programovacom rozhraní

Publikácia Virtuálne súkromné siete dokumentuje určené programovacie rozhrania umožňujúce klientovi písať programy, ktorými bude pristupovať k službám IBM i5/OS.

Ochranné známky

Nasledujúce pojmy sú ochrannými známkami spoločnosti International Business Machines Corporation v USA alebo iných krajinách:

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

Adobe, logo Adobe, PostScript a logo PostScript sú buď registrovanými ochrannými známkami alebo ochrannými známkami spoločnosti Adobe Systems Incorporated v USA a/alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochranné známky spoločnosti Microsoft Corporation v USA alebo iných krajinách.

Ostatné názvy spoločností, produktov a služieb môžu byť ochrannými známkami alebo servisnými známkami iných spoločností.

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a regulácie, vrátane všetkých zákonov a regulácií USA pre export.

SPOLOČNOSŤ IBM NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA