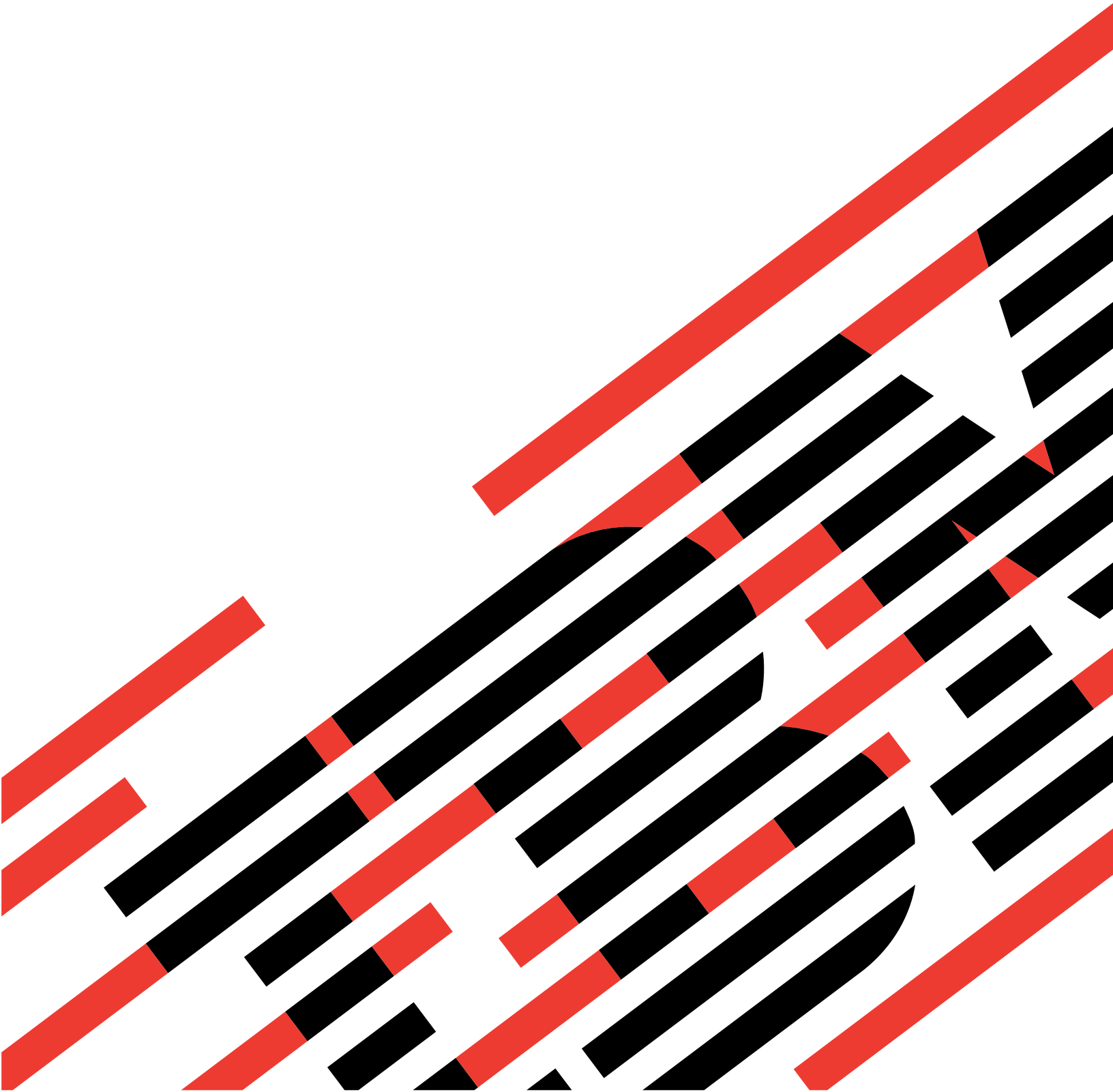
IBM

eserver

iSeries

Virtuálne súkromné siete

Verzia 5 Vydanie 3



IBM

@server

iSeries

Virtuálne súkromné siete

Verzia 5 Vydanie 3

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si prečítajte informácie v časti “Poznámky”, na strane 67.

Šieste vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 2 operačného systému IBM i5/OS (5722-SS1) a všetkých nasledujúcich vydaní a modifikácií, pokiaľ 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.

OS/400(R) VPN je voliteľne inštalovateľný komponent aplikácie iSeries(TM) Navigator, grafické užívateľské rozhranie (GUI) pre OS/400. Tento umožňuje vytvárať bezpečnú cestu medzi dvomi koncami medzi akoukoľvek kombináciou hostiteľa a brány. VPN pre OS/400 používa autentifikačné metódy, šifrovacie algoritmy a iné predbežné opatrenia na zaistenie, že údaje posielané medzi dvomi koncovými bodmi jej pripojenia budú neustále bezpečné.

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 vo V5R3
Táto téma opisuje, ktoré informácie sú v tomto vydaní nové alebo sa podstatne zmenili.

Vytlačenie tejto témy
Ak preferujete tlačenú verziu týchto informácií, prejdite sem a vytlačí sa PDF.

Návrhy VPN
Prejdite si tieto návrhy a oboznámte sa so základnými typmi VPN a krokmi potrebnými na ich konfiguráciu.

Koncepty VPN
Je dôležité, aby ste mali aspoň základné znalosti o štandardných technológiách VPN. Táto téma vám ponúka pojmové informácie o protokoloch, ktoré VPN používa vo svojej implementácii.

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.

Konfigurácia VPN
Po naplánovaní vašej VPN môžete pristúpiť k jej konfigurácii. Táto téma vám ponúka prehľad o tom, čo môžete robiť s VPN a ako to robiť.

Riadenie VPN
Táto téma popisuje rôzne úlohy, ktoré môžete vykonávať na správu vašich aktívnych pripojení VPN, vrátane toho, ako ich zmeniť, monitorovať alebo vymazať.

Odstraňovanie problémov s VPN
Na túto tému sa obráťte, keď zaznamenáte problémy s vašimi pripojeniami VPN.

Súvisiace informácie pre VPN
Tu nájdete odkazy na iné zdroje informácií o VPN a súvisiace témy.

Čo je nové vo V5R3

Funkčné vylepšenia
Vylepšenia funkcií virtuálnych súkromných sietí (VPN) vo verzii 5, vydaní 3 (V5R3) zahŕňajú dva nové typy identifikátorov. Sú to dva nové typy identifikátorov, ktoré môžu byť vybraté pri definovaní politík výmeny kľúčov VPN a koncových bodov spojenia. Tieto typy identifikátorov obsahujú lokálnu IP adresu a názov hostiteľa IPv4. Ďalšie informácie nájdete v online pomoci v iSeries(TM) Navigator.

- **Moja lokálna IP adresa**
  Identifikátor Moja lokálna IP adresa je možné vybrať na definovanie typu lokálneho servera kľúčov pre politiku Internet Key Exchange alebo lokálneho koncového bodu údajov v definícii pripojenia. Po vybratí VPN používa dostupnú adresu IPv4. Pripojenia VPN používajúce tento typ identifikátora nesmú používať filter politiky. Navyše musí byť lokálny systém iniciátorom pripojenia.
- **Názov hostiteľa IPv4**
  Identifikátor Názov hostiteľa IPv4 je možné vybrať na definovanie niekoľkých rôznych parametrov:
  – Identifikátor vzdialeného servera kľúčov v politike Internet Key Exchange
  – Identifikátor vzdialenej adresy vo vlastnostiach pripojenia
  – Definícia filtra politiky pre vlastnosti skupiny pripojení

  Názov hostiteľa IPv4 sa rozrieši na IP adresu hostiteľa zadaného ako typ identifikátora.

Oznámenie o bezpečnosti VPN:
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 na možný výskyt hesiel. Návod na nanútenie hlavného režimu dohodovania pre výmenu kľúčov nájdete v časti Zabezpečenie s autentifikáciou dopredu zdieľaného kľúča. Pri vytváraní alebo úprave politiky internetovej výmeny kľúčov môžete tiež použiť online pomoc aplikácie iSeries Navigator, kde nájdete potrebné podrobné informácie.

Informačné vylepšenia
Zmeny v téme informačného centra V5R3 VPN zahŕňajú vizuálnu prezentáciu vysvetľujúcu koncept tunela L2TP (Layer 2 Tunnel Protocol). Ak si chcete pozrieť vizuálnu prezentáciu o tuneloch L2TP zabezpečených pomocou IPSec, kliknite na nasledujúci odkaz. Toto vyžaduje Flash plug-in.

Prípadne môžete použiť HTML verziu tejto prezentácie.

Ako zistiť, čo je nové alebo zmenené

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

- Obrázok

  na označenie začiatku nových alebo zmenených informácií.
- Obrázok

  na označenie konca nových alebo zmenených informácií.

Keď chcete nájsť viac informácií o tom, čo je nové alebo zmenené v tomto vydaní, pozrite si dokument Memo to Users.

Vytlačiť túto tému

Ak si chcete prezrieť alebo stiahnuť PDF verziu tohto dokumentu, vyberte Virtuálna súkromná sieť (VPN) (približne 509 KB).

Ukladanie súborov PDF

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

1. Kliknite pravým tlačidlom na PDF vo vašom prehliadači (kliknite pravým tlačidlom na predchádzajúci odkaz).
2. Ak používate Internet Explorer, kliknite na **Save Target As...**. Ak používate Netscape Communicator, kliknite na **Save Link As...**
3. Prejdite do adresára, v ktorom si želáte uložiť PDF.
4. Kliknite na **Save**.

Sťahuje sa program Adobe Acrobat Reader

Na prezeranie a tlač týchto PDF potrebujete aplikáciu Adobe Acrobat Reader. Môžete si ju stiahnuť z webovej stránky spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html).

Návrhy VPN

Prezrite si nasledujúce návrhy, aby ste sa oboznámili s technickými a konfiguračnými podrobnosťami súvisiacimi s každým z týchto základných typov pripojení:

- **Návrh VPN: Základné pripojenie pobočky**
  V tomto scenári chce vaša spoločnosť vytvoriť VPN medzi podsieťami dvoch vzdialených oddelení cez pár počítačov iSeries(TM), ktoré fungujú ako brány VPN.
- **Návrh VPN: 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.
- **Návrh VPN: Ochrániť dobrovoľný tunel L2TP s IPSec**
  Tento návrh ilustruje pripojenie medzi hostiteľom pobočky a centrálou spoločnosti, ktorá používa L2TP chránený pomocou IPSec. Pobočka má dynamicky priradenú adresu IP, zatiaľ čo centrála spoločnosti má statickú, globálne smerovateľnú adresu IP.
- **Návrh VPN: Použiť preklad sieťových adries pre VPN**
  V tomto scenári si chce vaša spoločnosť vymeniť citlivé údaje s jedným z jej obchodných partnerov použitím OS/400(R) VPN. Pre ďalšiu ochranu sieťovej štruktúry vašej spoločnosti bude vaša spoločnosť používať aj VPN NAT na skrytie súkromnej adresy IP iSeries, ktorého používa na hosťovanie aplikácií, ku ktorým má obchodný partner prístup.

Viac návrhov VPN

Viac návrhov konfigurácie VPN nájdete v ostatných zdrojoch informácií pre VPN:

- **Návrh QoS: Bezpečné a predvídateľné výsledky (VPN a QoS)**
  S vašou VPN môžete vytvárať politiky typu kvalita služby (quality of service, QoS). Tento príklad ukazuje spoločné použitie oboch.
- **Virtuálne súkromné siete OS/400 V5R1: Vzdialený prístup k serveru IBM(R) e(logo)server iSeries Server s klientmi Windows(R) 2000 VPN, REDP0153**

  Táto publikácia IBM Redpaper poskytuje návod na konfiguráciu tunela VPN pomocou V5R1 VPN a integrovanej podpory L2TP a IPSec systému Windows 2000.

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

  Tento redbook skúma koncepty VPN a popisuje jej implementáciu pomocou bezpečnosti IP (IPSec) a Tunelovacieho protokolu vrstvy 2 (L2TP) na OS/400.
- **Bezpečnostné návrhy pre Internet pre AS/400: Praktický prístup, SG24-5954-00**

  Táto publikácia Redbook sa týka všetkých integrovaných komponentov sieťového zabezpečenia systému OS/400, ako sú IP filtre, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, audit a protokolovanie. Pomocou praktických príkladov popisuje ich použitie.

Návrh VPN: Základné pripojenie pobočky

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.

> **Dôležitá poznámka:**
> Tento scenár zobrazuje brány zabezpečenia iSeries(TM), ktoré sú priamo pripojené k internetu. Nie je tu firewall kvôli zjednodušeniu návrhu. Neznamená to, že použitie firewallu nie je nevyhnutné. Zvážte si bezpečnostné riziká pripojenia k internetu. Podrobné informácie o redukovaní týchto rizík nájdete v publikácii redbook AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00.

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.
- Používanie VPN poskytuje užívateľovi prístup ku všetkým serverom a prostriedkom na ktorejkoľvek strane pripojenia, ako keby boli pripojení pomocou prenajatej linky alebo pripojenia cez rozsiahlu sieť (Wide area network, WAN).
- 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

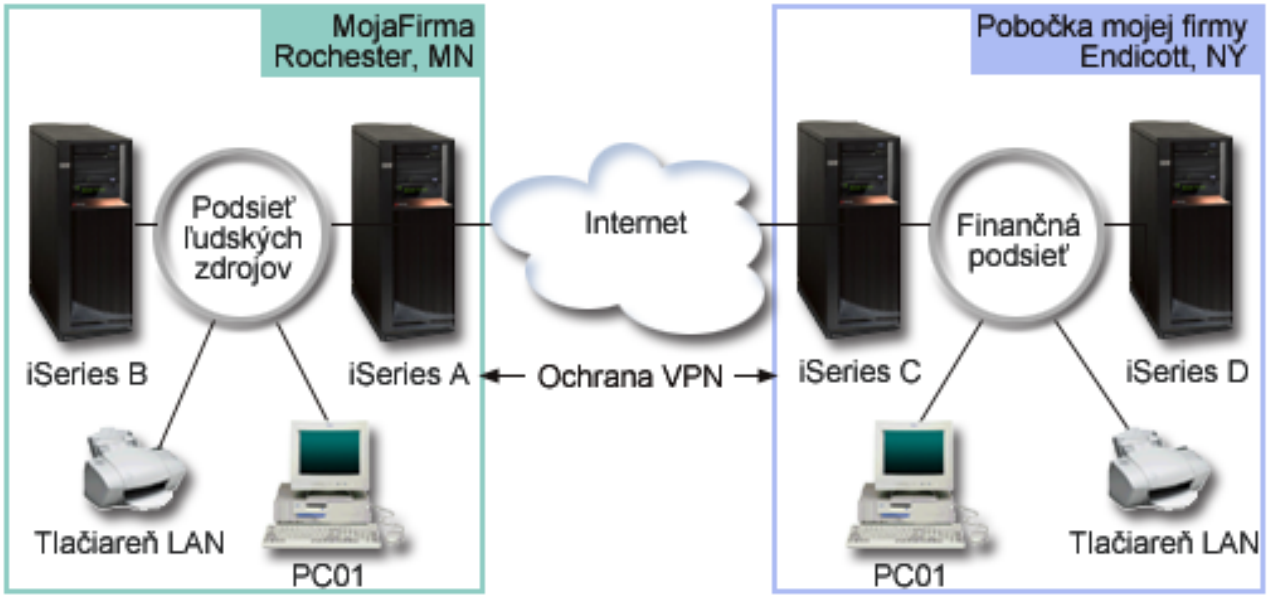
V tomto návrhu chce spoločnosť MyCo, Inc. vytvoriť VPN medzi podsieťami svojho Personálneho oddelenia a Finančného oddelenia cez dvojicu serverov iSeries. Oba servery budú slúžiť ako brány VPN. V termínoch konfigurácií VPN brána vykoná správu kľúčov a aplikuje IPSec na údaje, ktoré sa prenášajú tunelom. 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.
- Servery brán môžu vzájomne komunikovať a vzájomne pristupovať k svojim aplikáciám.

Podrobnosti

Nasledujúci obrázok ilustruje charakteristiky siete spoločnosti MyCo.



Personálne oddelenie

- iSeries-A beží na OS/400(R) verzia 5 vydanie 2 (V5R2) a funguje ako VPN brána 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.
- iSeries-A sa pripája na internet s adresou IP 204.146.18.227. Toto je koncový bod pripojenia. Teda iSeries-A vykonáva správu kľúčov a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP.
- iSeries-A sa pripája na svoju podsieť s adresou IP 10.6.11.1.
- iSeries-B je produkčný server v podsieti personálneho oddelenia, ktorý spúšťa štandardné aplikácie TCP/IP.

Finančné oddelenie

- iSeries-C pracuje na OS/400 verzie 5 vydaní 2 (V5R2) a funguje 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.
- iSeries-C sa pripája na internet s adresou IP 208.222.150.250. Toto je koncový bod pripojenia. Teda iSeries-C vykonáva správu kľúčov a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP.

- iSeries-C sa pripája na svoju podsieť s adresou IP 10.196.8.5.

Konfiguračné úlohy

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

1. Skontrolujte smerovanie TCP/IP, aby ste zaistili, že dva servery brány budú môcť navzájom komunikovať cez internet. Toto umožní zaistiť, že hostitelia na každej podsieti budú správne smerovať na svoju príslušnú bránu pre prístup na vzdialenú podsieť.
   Poznámka: Smerovanie je mimo oblasti tejto témy. V prípade otázok si pozrite smerovanie TCP/IP a nastavenie pracovného zaťaženia v informačnom centre.
2. Dokončite (stránka 6) plánovacie pracovné hárky a kontrolné zoznamy pre oba systémy.
3. Nakonfigurujte (stránka 7) VPN na bráne VPN Personálneho oddelenia (iSeries-A).
4. Nakonfigurujte (stránka 8) VPN na bráne VPN Finančného oddelenia (iSeries-C).
5. Overte, či sú servery VPN spustené (stránka 8).
6. Otestuje (stránka 8) komunikáciu medzi dvoma vzdialenými podsieťami.

Podrobnosti konfigurácie

Po dokončení prvého kroku ste zistili, či smerovanie TCP/IP funguje správne a vaše servery brán môžu komunikovať, môžete teda začať konfiguráciu VPN.

Krok 2: Vyplňte plánovacie pracovné hárky

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: Tieto pracovné hárky sa používajú pre iSeries-A, opakujú proces pre iSeries-C, pričom podľa potreby obracajú adresy IP.

Kontrolný zoznam predbežných podmienok	Odpovede
Je váš systém OS/400(R) V5R2 (5722-SS1) alebo novší?	Áno
Je nainštalovaná voľba Správca digitálnych certifikátov (5722-SS1 voľba 34)?	Áno
Je nainštalovaný Poskytovateľ šifrovaného prístupu (5722-AC2 alebo AC3)?	Áno
Je nainštalovaný iSeries(TM) Access for Windows(R) (5722-XE1)?	Áno
Je nainštalovaný iSeries Navigator?	Áno
Je nainštalovaný vedľajší komponent Sieť aplikácie iSeries Navigator?	Áno
Sú nainštalované pomocné programy pre pripojiteľnosť TCP/IP pre OS/400 (5722-TC1)?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Je na vašom iSeries nakonfigurovaný 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

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?	Nie 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

Krok 3: Nakonfigurujte VPN na iSeries-A

Na konfiguráciu VPN na iSeries-A použite informácie z pracovných hárkov, a to nasledujúcim spôsobom:

1. V aplikácii iSeries Navigator rozviňte iSeries-A **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Nové pripojenie.
3. Na stránke **Vítame vás** nájdete informácie o objektoch, ktoré vytvorí sprievodca.
4. Kliknite na **Ďalej** a prejdete na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte HRgw2FINgw.
6. (voliteľne) Zadajte popis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdete na stránku **Návrh pripojenia**.
8. Vyberte **Pripojiť vašu bránu na inú bránu**.
9. Kliknite na **Ďalej** a prejdete na stránku **Politika výmeny kľúčov cez Internet**.
10. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**.
11. Kliknite na **Ďalej** a prejdete na stránku **Certifikát pre lokálny koncový bod 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 prejdete 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 **dopredu zdieľaný 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 4 verzie IP** .

26. V poli **Identifikátor** zadajte 10.196.8.0.
27. V poli **Maska podsiete** zadajte 255.255.255.0.
28. Kliknite na **Ďalej** a prejdete na stránku **Údajové služby**.
29. Prijmite predvolené hodnoty, potom kliknite na **Ďalej** a prejdete na stránku **Údajová politika**.
30. Vyberte **Vytvoriť novú politiku**, potom vyberte **Vyvážiť bezpečnosť a výkon**. Vyberte **Použiť šifrovací algoritmus RC4**.
31. Kliknite na **Ďalej** a prejdete na stránku **Použiteľné rozhrania**.
32. V tabuľke **Linka** vyberte **TRLINE**.
33. Kliknite na **Ďalej** a prejdete na stránku **Súhrn**. Prezrite objekty, ktoré vytvorí sprievodca a presvedčte sa, či sú správne.
34. Kliknutím na **Dokončiť** dokončite konfiguráciu.
35. Keď sa objaví dialógové okno **Aktivovať filtre politík**, vyberte **Áno, aktivovať vygenerované filtre politík** a **Povoliť všetky ďalšie prenosy**. Kliknutím na **OK** dokončíte konfiguráciu. Po výzve zadajte, že chcete aktivovať pravidlá na všetkých rozhraniach.

Teraz ste dokončili konfiguráciu VPN na iSeries-A. Ďalším krokom bude konfigurácia VPN na bráne VPN Finančného oddelenia (iSeries-C).

Krok 4: Nakonfigurujte VPN na iSeries-C

Postupujte podľa tých istých krokov, ktoré ste použili na konfiguráciu iSeries-A, pričom podľa potreby obráťte adresy IP. Ako vodidlo použite plánovacie pracovné hárky. 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.

Krok 6: Spustite servery VPN

Ak chcete spustiť servery VPN, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **Server —> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a zvoľte **Spustiť**.

Krok 7: Otestujte pripojenie

Po dokončení konfigurácie obidvoch serverov a po úspešnom spustení VPN serverov otestujte konektivitu, aby ste sa uistili, že vzdialené podsiete môžu navzájom komunikovať. Za týmto účelom postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **iSeries-A —>Sieť**.
2. Kliknite pravým tlačidlom na **konfigurácia TCP/IP** a zvoľte **Pomocné programy**, potom zvoľte **Ping**.
3. Z dialógového okna **Ping z** zadajte iSeries-C do poľa **Ping**.
4. Kliknite na **Vykonať ping teraz** na overenie konektivity z iSeries-A na iSeries-C.
5. Keď skončíte, kliknite na **OK**.

Návrh VPN: Základné medzipodnikové pripojenie

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 ľahší, 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. Pomocou verejného internetu môžete jednoducho vytvoriť virtuálnu súkromnú sieť (Virtual private network, VPN), ktorá bude vyhovovať potrebám oboch spoločností.

Ciele

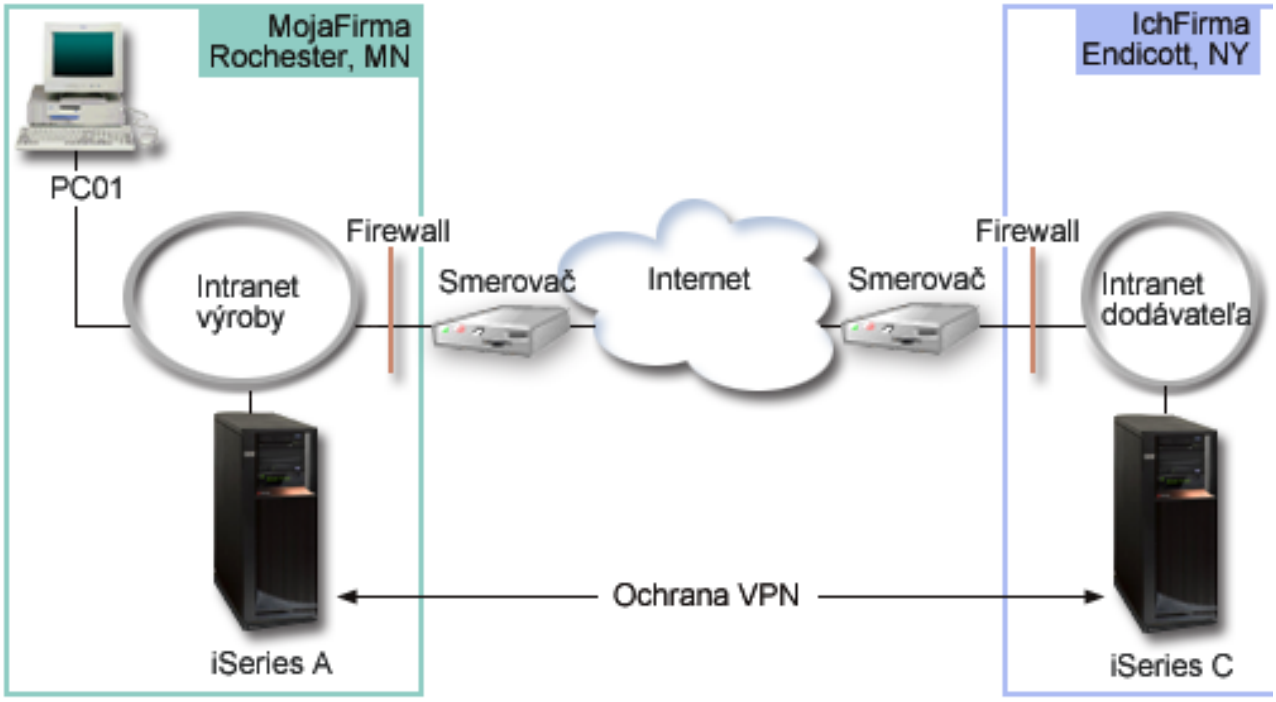
V tomto návrhu chce spoločnosť MyCo vytvoriť VPN medzi hostiteľom vo svojej divízii súčiastok a hostiteľom vo výrobnom oddelení jedného zo svojich obchodných spoločníkov, TheirCo.

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.

Dôležitá poznámka:
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.

Podrobnosti

Nasledujúci obrázok ilustruje charakteristiky siete spoločnosti MyCo a TheirCo.



Sieť zásobovania MyCo

- iSeries-A beží na OS/400(R) verzia 5 vydanie 2 (V5R2).
- iSeries-A má adresu IP 10.6.1.1. Toto je koncový bod pripojenia, ako aj koncový bod údajov. Teda iSeries-A vykonáva vyjednávania IKE a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP a je aj zdrojom a cieľom pre údaje, ktoré obiehajú cez VPN.
- iSeries-A je v podsieti 10.6.0.0 s maskou 255.255.0.0
- Len iSeries-A môže zahájiť pripojenie s iSeries-C.

Sieť výroby TheirCo

- iSeries-C pracuje na OS/400 verzie 5 vydaní 2 (V5R2).
- iSeries-C má adresu IP 10.196.8.6. Toto je koncový bod pripojenia, ako aj koncový bod údajov. Teda iSeries-A vykonáva vyjednávania IKE a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP a je aj zdrojom a cieľom pre údaje, ktoré obiehajú cez VPN.
- iSeries-C je v podsieti 10.196.8.0 s maskou 255.255.255.0

Konfiguračné úlohy

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

1. Skontrolujte smerovanie TCP/IP, aby ste zaistili, že iSeries-A a iSeries-C budú môcť navzájom komunikovať cez internet. Toto zaistí, že hostitelia na každej podsieti budú správne smerovať na svoju príslušnú bránu pre prístup na vzdialenú podsieť. Buďte si vedomý toho, že pre tento scenár budete potrebovať zvážiť smerovanie súkromných adries, ktoré ste predtým nemali.

   Poznámka: Smerovanie je mimo oblasť tejto témy. V prípade otázok si pozrite Informačné centrum TCP/IP routing and workload balancing.
2. Dokončite (stránka 10) plánovacie pracovné hárky a kontrolné zoznamy pre oba systémy.
3. Nakonfigurujte (stránka 11) VPN na iSeries-A v sieti zásobovania spoločnosti MyCo.
4. Nakonfigurujte (stránka 11) VPN na iSeries-C v sieti výroby spoločnosti TheirCo.
5. Aktivujte (stránka 12) pravidlá pre filtre na oboch serveroch.
6. Spustite (stránka 12) pripojenie z iSeries-A.
7. Otestuje (stránka 13) komunikáciu medzi dvoma vzdialenými podsieťami.

Podrobnosti konfigurácie

Keď dokončíte prvý krok, overili ste, či smerovanie TCP/IP funguje správne a vaše servery môžu komunikovať, môžete začať konfiguráciu VPN.

Krok 2: Vyplňte plánovacie pracovné hárky

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: Tieto pracovné hárky sa používajú pre iSeries-A, opakujú proces pre iSeries-C, pričom podľa potreby obracajú adresy IP.

Kontrolný zoznam predbežných podmienok	Odpovede
Je váš systém OS/400(R) V5R2 (5722-SS1) alebo novší?	Áno
Je nainštalovaná voľba Správca digitálnych certifikátov (5722-SS1 voľba 34)?	Áno
Je nainštalovaný Poskytovateľ šifrovaného prístupu (5722-AC2 alebo AC3)?	Áno
Je nainštalovaný iSeries(TM) Access for Windows(R) (5722-XE1)?	Áno
Je nainštalovaný iSeries Navigator?	Áno
Je nainštalovaný vedľajší komponent Sieť aplikácie iSeries Navigator?	Áno
Sú nainštalované pomocné programy pre pripojiteľnosť TCP/IP pre OS/400 (5722-TC1)?	Áno
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	Áno
Je na vašom iSeries nakonfigurovaný 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

Kontrolný zoznam predbežných podmienok	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

Na konfiguráciu VPN budete potrebovať tieto informácie	Odpovede
Aký typ pripojenia vytvárate?	hostiteľ-hostiteľ
Ako pomenujete skupinu dynamických kľúčov?	MyCo-TheirCo
Ak typ bezpečnosti a výkonu systému vyžadujete na ochranu vašich kľúčov?	najvyššiu
Používate certifikáty na autentifikáciu pripojenia? Ak nie, aký je dopredu zdieľaný kľúč?	Áno
Aký je identifikátor lokálneho servera kľúčov?	Adresa IP: 10.6.1.1
Aký je identifikátor lokálneho koncového bodu údajov?	Adresa IP: 10.6.1.1
Aký je identifikátor vzdialeného servera kľúčov?	Adresa IP: 10.196.8.6
Aký je identifikátor vzdialeného koncového bodu údajov?	Adresa IP: 10.196.8.6
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

Krok 3: Nakonfigurujte VPN na iSeries-A

Na konfiguráciu VPN na iSeries-A použite informácie z pracovných hárkov, a to nasledujúcim spôsobom:

1. V aplikácii iSeries Navigator rozviňte váš server **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Nové pripojenie**, čím spustíte sprievodcu Pripojenie.
3. Na stránke **Vítame vás** nájdete informácie o tom, ktoré objekty vytvorí sprievodca.
4. Kliknite na **Ďalej** a prejdete na stránku **Názov pripojenia**.
5. V poli **Názov** zadajte MyCo-TheirCo.
6. (voliteľne) Zadajte popis pre túto skupinu pripojení.
7. Kliknite na **Ďalej** a prejdete na stránku **Návrh pripojenia**.
8. Vyberte **Pripojiť vášho hostiteľa na iného hostiteľa**.
9. Kliknite na **Ďalej** a prejdete na stránku **Politika výmeny kľúčov cez Internet**.
10. Vyberte **Vytvoriť novú politiku**, potom vyberte **Najvyššia bezpečnosť, najnižší výkon**.
11. Kliknite na **Ďalej** a prejdete na stránku **Certifikát pre lokálny koncový bod pripojenia**.
12. Vyberte **Áno** na označenie, že budete používať certifikáty na autentifikáciu pripojenia. Potom vyberte certifikát, ktorý reprezentuje iSeries-A.
    Poznámka: Ak chcete používať certifikát na autentifikáciu lokálneho koncového bodu pripojenia, najskôr musíte vytvoriť 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 prejdete 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 prejdete na stránku **Údajové služby**.
19. Prijmite predvolené hodnoty, potom kliknite na **Ďalej** a prejdete na stránku **Údajová politika**.
20. Vyberte **Vytvoriť novú politiku**, potom vyberte **Najvyššia bezpečnosť, najnižší výkon**. Vyberte **Použiť šifrovací algoritmus RC4**.
21. Kliknite na **Ďalej** a prejdete 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**.

Ďalší krok je na určenie, že len iSeries-A môže zahájiť toto pripojenie. 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. Kliknite na **OK** a vaše zmeny sa uložia.

Teraz ste dokončili konfiguráciu VPN na iSeries-A. Ďalším krokom bude konfigurácia VPN na iSeries-C v sieti výroby TheirCo.

Krok 4: Nakonfigurujte VPN na iSeries-C

Postupujte podľa tých istých krokov, ktoré ste použili na konfiguráciu iSeries-A, pričom podľa potreby obráťte adresy IP. Ako vodidlo použite plánovacie pracovné hárky. Keď dokončíte konfiguráciu iSeries-C, musíte aktivovať pravidlá pre filtre, ktoré sprievodca Pripojenie vytvoril na každom serveri.

Krok 5: Aktivujte pravidlá pre pakety

Sprievodca automaticky vytvorí pravidlá pre pakety, ktoré toto pripojenie vyžaduje, aby mohol správne pracovať. Ale než budete môcť spustiť pripojenie VPN, musíte ich aktivovať na oboch systémoch. Ak to chcete vykonať na iSeries-A, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **iSeries-A> Sieť—> Politiky IP**.
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. Zopakujte tieto kroky na aktiváciu pravidiel pre pakety na iSeries-C.

Krok 6: Spustite pripojenie

Ak chcete spustiť pripojenie MyCo-TheirCo z iSeries-A, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **iSeries-A> Sieť—> Politiky IP**.
2. Ak nie je server VPN spustený, kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Spustiť**. Takto spustíte server VPN.
3. Rozviňte **Virtuálne súkromné siete —>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*. Spustenie pripojenia môže trvať niekoľko minút, takže pravidelne obnovujte, kým sa stav nezmení na *Povolený*.

Krok 7: Otestujte pripojenie

Po dokončení konfigurácie obidvoch serverov a po úspešnom pripojení serverov otestujte konektivitu, aby ste sa uistili, že vzdialení hostitelia môžu navzájom komunikovať. Za týmto účelom postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **iSeries-A —>Sieť**.
2. Kliknite pravým tlačidlom na **konfigurácia TCP/IP** a vyberte **Pomocné programy**, potom vyberte **Ping**.
3. Z dialógového okna **Ping z** zadajte iSeries-C do poľa **Ping**.
4. Kliknite na **Vykonať ping teraz** na overenie konektivity z iSeries-A na iSeries-C.
5. Keď skončíte, kliknite na **OK**.

Návrh VPN: Ochrániť dobrovoľný tunel L2TP s IPSec

Predpokladajme, že vaša spoločnosť má malú pobočku v inom štáte. Počas ľubovoľného daného pracovného dňa môže táto pobočka žiadať o prístup k utajeným informáciám o iSeries(TM) v rámci vášho podnikového intranetu. 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 sa chcete dozvedieť viac o konceptoch L2TP, pozrite si Layer 2 Tunnel Protocol (L2TP).

> **Dôležitá poznámka:**
> Tento návrh ukazuje bezpečnostné brány iSeries pripojené priamo na Internet. 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. Podrobné informácie o redukovaní týchto rizík nájdete v publikácii redbook AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00.

Ciele

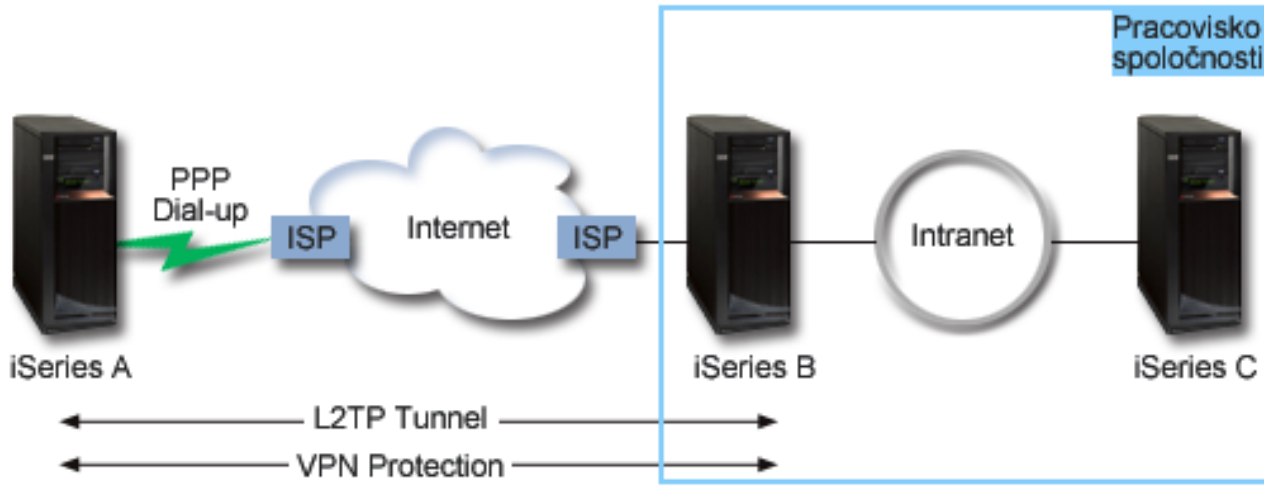
V tomto návrhu sa pobočka iSeries pripája na svoju podnikovú sieť cez bránu iSeries s tunelom L2TP chráneným pomocou VPN.

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.

Podrobnosti

Nasledujúci obrázok ilustruje charakteristiky siete pre tento návrh.



iSeries-A

- Musí mať prístup k aplikáciám TCP/IP na všetkých systémoch v podnikovej sieti.
- Prijíma dynamicky priradené adresy IP od svojho ISP.
- Musí byť nakonfigurovaný na poskytovanie podpory L2TP.

iSeries-B

- Musí mať prístup k aplikáciám TCP/IP na iSeries-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. Teda iSeries-B vykonáva správu kľúčov a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP. iSeries-B sa pripája na svoju podsieť s adresou IP 10.6.11.1.

V termínoch L2TP, *iSeries-A* sa správa ako iniciátor L2TP, zatiaľ čo *iSeries-B* sa správa ako terminátor L2TP.

Konfiguračné úlohy

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

1. Nakonfigurovať VPN (stránka 14) na iSeries-A.
2. Nakonfigurovať profil pripojenia PPP (stránka 16) a virtuálnu linku pre iSeries-A.
3. Použiť (stránka 17) skupinu dynamických kľúčov na profil PPP.
4. Nakonfigurovať VPN (stránka 17) na iSeries-B.
5. Nakonfigurovať profil pripojenia PPP (stránka 16) a virtuálnu linku pre iSeries-B.
6. Aktivovať (stránka 18) pravidlá pre pakety na iSeries-A a iSeries-B.
7. Spustite (stránka 19) pripojenie z iSeries-A.

Podrobnosti konfigurácie

Po skontrolovaní správnej funkčnosti TCP/IP a schopnosti komunikácie vašich serverov iSeries(TM) ste pripravený začať konfigurovať pripojenie opísané v tomto scenári.

Krok 1: Nakonfigurujte VPN na iSeries-A

Ak chcete nakonfigurovať VPN na iSeries-A, postupujte podľa týchto krokov:

1. **Nakonfigurovať politiku Internet Key Exchange**

a. V aplikácii iSeries Navigator rozviňte iSeries-A —> **Sieť**—> **Politiky IP**—> **Virtuálne súkromné siete**—> **Bezpečnostné politiky IP**.
b. Kliknite pravým tlačidlom 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 totojeidkluca. Nezabudnite, že lokálny server kľúčov má dynamický priradenú adresu IP, ktorú nemožno vedieť dopredu. iSeries-B používa tento identifikátor na identifikáciu iSeries-A, keď iSeries-A zahajuje pripojenie.
g. Na stránke **Transformácie** kliknutím na **Pridať** pridáte transformácie, ktoré iSeries-A navrhuje iSeries-B pre ochranu kľúčov a na určenie, či politika IKE používa ochranu totožnosti pri zahajovaní vyjednávaní fázy 1.
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 (žiadna ochrana identifikácie).**

»

Poznámka: Ak používate vo svojej konfigurácii spolu dopredu zdieľané kľúče a agresívny režim dohadovania, vyberte hesiel, pre ktoré nebude jednoduché odhalenie pri narušeniach, ktoré skenujú slovník. 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 kliknite pravým tlačidlom na **Údajové politiky** a vyberte **Nová údajová politika**.
   b. Na stránke **Všeobecné** zadajte názov údajovej politiky. Napríklad l2tpvzdialuziv.
   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** a pridáte transformáciu údajovej politiky.
   e. Vyberte **Prenos** pre režim zapuzdrenia.
   f. Zadajte hodnotu pre ukončenie platnosti kľúča.
   g. Kliknite na **OK** a vrátite sa na stránku **Transformácie**.
   h. Kliknite na **OK** a vaša nová údajová politika sa uloží.
3. **Nakonfigurovať skupinu dynamických kľúčov**
4.
   a. V rozhraní VPN rozviňte **Bezpečné pripojenia**.
   b. Kliknite pravým tlačidlom 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**. Z rozbaľovacieho zoznamu **Údajová politika** vyberte údajovú politiku, ktorú ste vytvorili v kroku dva, l2tpvzdialuziv.

g. Vyberte **Lokálny systém zahajuje pripojenie** na označenie, že len iSeries-A môže zahájiť pripojenia s iSeries-B.

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.

Teraz musíte pridať pripojenie do skupiny, ktorú ste práve vytvorili.

5. **Nakonfigurovať pripojenie dynamických kľúčov**

a. V rozhraní VPN rozviňte **Podľa skupiny**. Zobrazí sa zoznam všetkých skupín dynamických kľúčov, ktoré ste nakonfigurovali na iSeries-A.

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. V rozbaľovacom zozname **Protokol** vyberte **UDP**.

l. Kliknutím na **OK** vytvoríte pripojenie dynamických kľúčov.

Teraz ste dokončili konfiguráciu VPN na iSeries-A. Ďalším krokom je konfigurácia profilu PPP pre iSeries-A.

Krok 2: Nakonfigurujte profil pripojenia PPP a virtuálnu linku na iSeries-A

Táto časť popisuje kroky, ktoré musíte vykonať na vytvorenie profilu PPP pre iSeries-A. Profil PPP nemá k sebe priradenú žiadnu fyzickú linku. Namiesto toho používa virtuálnu linku. To preto, lebo prenos PPP prechádza tunelom L2TP, zatiaľ čo VPN ochraňuje tunel L2TP.

Ak chcete vytvoriť profil pripojenia PPP pre iSeries-A, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte iSeries-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. (voliteľne) Zadajte popis pre tento 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 **Názov lokálneho hostiteľa** zadajte názov hostiteľa pre lokálny server kľúčov, iSeriesA.
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 z rozbaľovacieho zoznamu **Názov skupiny pripojení** vyberte skupinu dynamických kľúčov, ktorú ste vytvorili v kroku jedna, l2tptocorp.
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 v profile PPP nie sú k dispozícii žiadne informácie o smerovaní, iSeries-A bude schopný dosiahnuť len koncový bod vzdialeného systému, ale žiadne iné systémy na 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, ktorý sa má použiť** vyberte **Vyžadovať šifrované heslo (CHAP-MD5)**
28. Zadajte meno užívateľa, iSeriesA, a heslo.
29. Kliknite na **OK** a uložíte profil PPP.

Krok 3: Použite skupinu dynamických kľúčov l2tptocorp na profil 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. Za týmto účelom postupujte podľa týchto krokov:

1. Prejdite na rozhranie VPN a rozviňte **Bezpečné pripojenia—>Podľa skupiny**.
2. Kliknite pravým tlačidlom na skupinu dynamických kľúčov, l2tptocorp, a vyberte **Vlastnosti**.
3. Prejdite na stránku **Rozhrania** a vyberte **Použiť túto skupinu** pre profil PPP, ktorý ste vytvorili v kroku dva, toCorp.
4. Kliknutím na **OK** použijete l2tptocorp na profil PPP, toCorp.

Krok 4: Nakonfigurujte VPN na iSeries-B

Postupujte podľa tých istých krokov, ktoré ste použili na konfiguráciu iSeries-A, pričom podľa potreby obráťte adresy IP a identifikátory. Kým začnete vezmite do úvahy tieto ďalšie body:

- Identifikujte vzdialený server kľúčov podľa identifikátora kľúča, ktorý ste zadali pre lokálny server kľúčov na iSeries-A. Napríklad totojeidkluca.
- Použite *presne* tie isté dopredu zdieľané kľúče.
- Skontrolujte, či sa transformácie zhodujú s tými, ktoré ste nakonfigurovali na iSeries-A, inak pripojenia zlyhajú.
- 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.

Krok 5: Nakonfigurujte profil pripojenia PPP a virtuálnu linku na iSeries-B

Ak chcete vytvoriť profil pripojenia PPP pre iSeries-B, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte iSeries-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. (voliteľne) Zadajte popis pre tento 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 pre lokálny server kľúčov, iSeriesB.
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, ktorý sa má použiť** vyberte **Vyžadovať šifrované heslo (CHAP-MD5)**
23. Zadajte meno užívateľa, iSeriesB, a heslo.
24. Kliknite na **OK** a uložíte profil PPP.

Krok 6: Aktivujte pravidlá pre pakety

VPN automaticky vytvorí pravidlá pre pakety, ktoré toto pripojenie vyžaduje, aby mohol správne pracovať. Ale než budete môcť spustiť pripojenie VPN, musíte ich aktivovať na oboch systémoch. Ak to chcete vykonať na iSeries-A, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte **iSeries-A> Sieť—> Politiky IP**.

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. Zopakujte tieto kroky na aktiváciu pravidiel pre pakety na iSeries-B.

Krok 7: Spustite pripojenie

Posledným krokom je spustenie pripojenia. Kým budete môcť zahájiť pripojenie L2TP, musíte povoliť terminátoru L2TP odpovedať na požiadavky iniciátora. Keď skontrolujete, či sú spustené všetky vyžadované služby, spustite pripojenie PPP na strane terminátora. Nasledujúce kroky popisujú, ako spustiť pripojenie PP na iSeries-B:

1. V aplikácii iSeries Navigator rozviňte iSeries-B **—> Sieť—> Služby vzdialeného prístupu**.
2. Kliknite na **Profily pripojenie respondenta** a v pravom okne sa zobrazí zoznam profilov respondenta.
3. Kliknite pravým tlačidlom na tobranch a vyberte **Spustiť**. Po spustení profilu pripojenia sa okno obnoví a zobrazí pripojenie ako Čaká na požiadavky o pripojenie. iSeries-A môže teraz odpovedať na požiadavky o pripojenie L2TP z iSeries-B.

Ak chcete spustiť pripojenie L2TP na iSeries-A, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte iSeries-A **—> Sieť—> Služby vzdialeného prístupu**.
2. Kliknite na **Profily pripojenie pôvodcu** a v pravom okne sa zobrazí zoznam profilov respondenta.
3. Kliknite pravým tlačidlom na **toCORP** a vyberte **Spustiť**. Po spustení profilu pripojenia sa okno obnoví a zobrazí pripojenie ako Vytvára sa tunel L2TP.
4. Stlačením F5 obnovte obrazovku. Ak sa tunel L2TP spustil úspešne, stav pripojenia bude uvádzať Aktívne pripojenia.

Scenár VPN: Použiť preklad sieťových adries pre VPN

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. Pre ďalšiu ochranu vašej podnikovej siete ste sa rozhodli, že potrebujete skryť súkromnú IP adresu iSeries(TM), ktorý hostí aplikácie ku ktorým má dodávateľ prístup. Otázka znie: Ako zariadite, aby to fungovalo?

Odpoveď: OS/400(R) VPN. Použite ju nielen na vytvorenie definícií pripojenia na bráne VPN v sieti vašej spoločnosti, ale aj na zabezpečenie prekladu adries, ktoré potrebujte sa skrytie svojich 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.

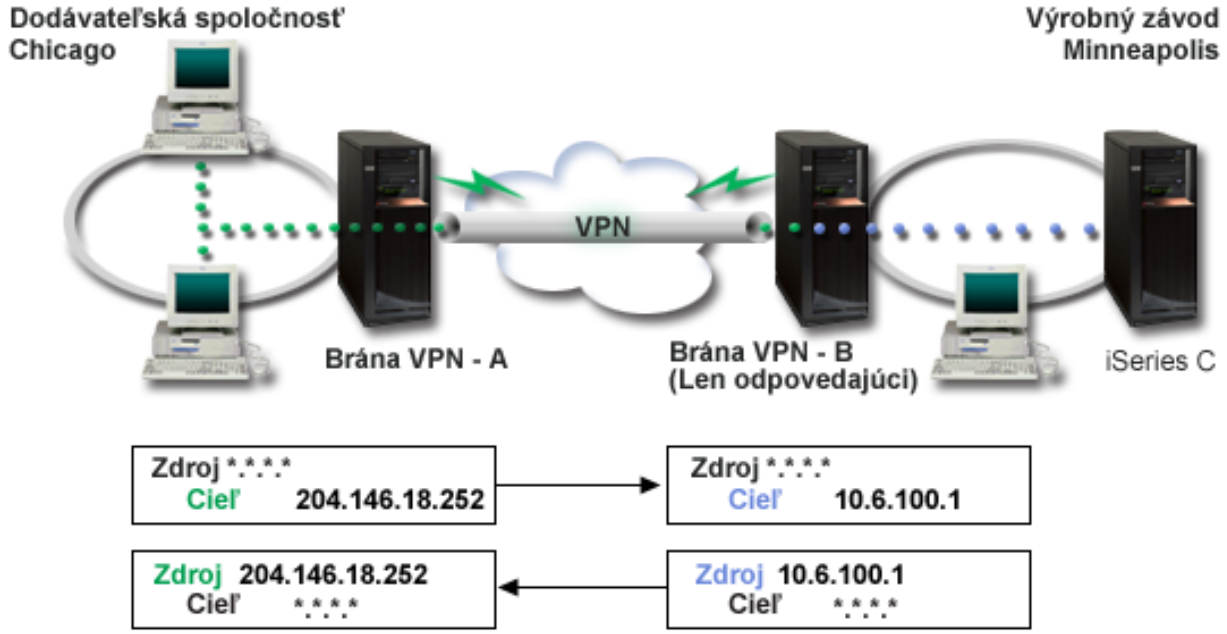
Ciele

Ciele tohto scenára sú nasledovné:

- umožniť všetkým klientom v sieti dodávateľa prístup na jedného hostiteľa iSeries v sieti výrobcu cez pripojenie VPN typu brána-brána.
- skryť súkromnú adresu IP hostiteľského iSeries v sieti výrobcu pomocou jej prekladu na verejnú adresu IP pomocou prekladu sieťových adries VPN (VPN NAT).

Podrobnosti

Nasledujúci obrázok ilustruje sieťovú charakteristiku siete dodávateľa aj siete výrobcu:



- Brána-A VPN sa nakonfiguruje tak, aby vždy zahajovala pripojenia na bránu-B VPN.
- Brána-A VPN definuje cieľový koncový pre pripojenie ako 204.146.18.252 (verejná adresa priradená k iSeries-C).
- iSeries-C má súkromnú adresu IP v sieti výrobcu 10.6.100.1.
- Verejná adresa 204.146.18.252 bola definovaná v lokálnej servisnej oblasti na bráne-B VPN pre súkromnú adresu servera iSeries-C, 10.6.100.1.
- Brána-B VPN preloží verejnú adresu servera iSeries-C na jeho súkromnú adresu, 10.6.100.1, pre vstupné datagramy. Brána-B VPN preloží vracajúce sa výstupné datagramy z 10.6.100.1 späť na verejnú adresu servera iSeries-C, 204.146.18.252. Pokiaľ ide o klientov v sieti dodávateľa, iSeries-C má adresu IP 204.146.18.252. Títo nebudú nikdy upozornení na to, že nastal preklad adresy.

Konfiguračné úlohy

Ak chcete nakonfigurovať pripojenie popísané v tomto scenári, musíte vykonať každú z nasledujúcich úloh:

1. Nakonfigurovať základnú VPN typu brána-brána medzi **Bránou-A VPN** a **Bránou-B** VPN.
2. Definovať lokálnu servisnú oblasť na **Bráne-B VPN** na skrytie súkromnej adresy servera **iSeries-C** za verejný identifikátor, 204.146.18.252.
3. Nakonfigurovať **Bránu-B VPN** na preklad lokálnych adries pomocou adries lokálnej servisnej oblasti.

Koncepty VPN

Virtuálne súkromné siete (VPN) používajú na ochranu prenosu údajov niekoľko dôležitých protokolov TCP/IP. Pre lepšie pochopenie spôsobu fungovania pripojenia VPN sa oboznámte s týmito protokolmi, konceptmi a so spôsobom akým ich OS/400(R) VPN používa:

- **Protokoly Bezpečnosti IP (IPSec)**
  IPSec zabezpečuje stabilný, dlhotrvajúci základ na poskytovanie bezpečnosti sieťovej vrstvy.

- **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.
- **Tunelovací protokol vrstvy 2 (L2TP)**
  Ak plánujete používať pripojenie VPN na zabezpečenie komunikácie medzi vašou sieťou a vzdialenými klientmi, musíte sa oboznámiť aj s L2TP.
- **Preklad sieťových adries pre VPN (VPN NAT)**
  VPN pre OS/400 zabezpečuje prostriedky na vykonávanie prekladu sieťových adries, nazývané 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.
- **Zapuzdrenie UDP**
  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.
- **Komprimácia IP (IPComp)**
  IPComp zmenšuje veľkosť datagramov IP pomocou komprimácie datagramov na zvýšenie komunikačného výkonu medzi partnermi VPN.
- **VPN a filtrovanie 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.

Bezpečnostné protokoly IP (IPSec)

IPSec zabezpečuje stabilný, dlhotrvajúci základ na poskytovanie bezpečnosti sieťovej vrstvy. Podporuje všetky šifrovacie algoritmy, ktoré sa v súčasnosti používajú a môže sa prispôsobiť aj novším, výkonnejším algoritmom, keď budú k dispozícii. 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.
Dôvernosť údajov
Utajuje obsah správy, väčšinou pomocou šifrovania.
Ochrana opakovaného prehrávania
Zaisťuje, že útočník nemôže zachytiť datagram a prehrať ho niekedy neskôr.
Automatizovaná správa šifrovacích kľúčov a bezpečnostných asociácií
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.

Nasledujú základné protokoly IPSec:

- **Protokol Authentication Header (AH)**
- **Protokol Encapsulating Security Payload (ESP)**
- **Kombinácia protokolov AH a ESP**
- **Protokoly Internet Key Exchange (IKE)**

Internet Engineering Task Force (IETF) formálne definuje IPSec v Požiadavke o komentár (Request for Comment, RFC) 2401, *Bezpečnostná architektúra pre Internetový protokol*. Túto RFC nájdete na Internete na nasledujúcej webovej stránke: 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. Pre zaistenie autentifikácie pôvodu údajov obsahuje AH v algoritme tajný zdieľaný kľúč, ktorý sa používa na autentifikáciu. Pre zaistenie ochrany opakovaného prehrávania, AH používa v hlavičke AH pole sekvenčného čísla. Tieto tri rozdielne funkcie sa často dávajú dokopy a spolu tvoria **autentifikácia**. Jednoducho povedané, AH zaisťuje, že s vašimi údajmi sa počas trasy do ich konečného cieľa nepovolene nemanipulovalo.

Hoci AH, pokiaľ ide o datagram IP, autentifikuje podľa možností maximum, hodnoty istých polí v hlavičke IP nemôže príjemca predvídať. AH tieto polia, známe ako **premenlivé** polia, neochraňuje. 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*. Túto RFC nájdete na Internete na nasledujúcej webovej stránke: 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. Napríklad dve bezpečnostné brány môžu fungovať ako tunel AH na autentifikáciu celkovej prevádzky 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 práve AH?

V mnohých prípadoch vyžadujú vaše údaje len autentifikáciu. Zatiaľ čo protokol Encapsulating Security Payload (ESP) môže vykonávať autentifikáciu, AH neovplyvní výkon systému tak ako ESP. 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 v niektorých krajinách obmedzené, kým AH nie je regulované a môže sa voľne používať na celom svete.

Aký algoritmus používa AH na ochranu informácií?

AH používa algoritmus, známy ako **autentifikačné kódy transformovanej správy (hashed message authentication codes, HMAC)**. 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*. Toto RFC nájdete na internete na nasledujúcej webovej stránke: 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 ESP a protokolom Autentifikačná hlavička (Authentication Header, AH) je, že ESP zabezpečuje šifrovanie, zatiaľ čo oba protokoly zabezpečujú 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 potencionáným 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. OS/400(R) VPN používa na šifrovanie DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 alebo AES (Advanced Encryption Standard).

Internet Engineering Task Force (IETF) formálne definuje DES v Požiadavke o komentár (Request for Comment, RFC) 1829, *Transformácia ESP DES-CBC*. Internet Engineering Task Force (IETF) formálne definuje 3DES v RFC 1851, *Transformácia ESP trojitým DES*. Tieto a iné RFC nájdete na Internete na nasledujúcej webovej adrese: 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.

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 a iné RFC nájdete na Internete na nasledujúcej webovej adrese: 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. Hoci kombinácia týchto dvoch protokolov poskytuje väčšiu bezpečnosť, dodatočné spracovanie môže znížiť efekt úžitku.

Správa kľúčov

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 IBM(TM) implementácia protokolu IKE (Internet Key Exchange). 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 správy 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. Svoje digitálne certifikáty musíte nakonfigurovať pomocou Správcu digitálnych certifikátov (5722-SS1 voľba 34). Okrem toho niektoré riešenia VPN vyžadujú pre prevádzkyschopnosť Podpis RSA. Napríklad Windows(R) 2000 VPN používa RSA podpis ako svoju štandardnú

autentifikačnú metódu. 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.

Pri vytvorení dynamickej VPN pomocou aplikácie iSeries(TM) Navigator musíte zadefinovať politiku IKE na povolenie vyjednávaní fázy 1 a údajovú politiku na riadenie vyjednávania 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.

Navrhované 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)*

Toto RFC nájdete na Internete na nasledujúcej webovej stránke: http://www.rfc-editor.org.

Tunelový protokol vrstvy 2 (L2TP)

Pripojenia tunelovacieho protokolu vrstvy 2 (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 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. Na dobrovoľnom tuneli končí tunel na vzdialenom klientovi, zatiaľ čo povinný tunel končí na ISP.

S **povinným tunelom** L2TP vzdialený hosť inicializuje pripojenie na svojho Poskytovateľa internetových služieb (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. Scenár *Ochrana tunela L2TP pomocou IPSec* vám poskytuje príklad konfigurácie pobočkových iSeries(TM) na pripojenie k podnikovej sieti cez bránu iSeries pomocou tunela L2TP zabezpečeného pomocou VPN.

Môžete si pozrieť vizuálne prezentácie o koncepte Tunelov L2TP zabezpečených pomocou IPSec. Toto vyžaduje Flash plug-in.

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).

Pozrite si Scenár: Konfigurácia vzdialeného PPP komutovaného pripojenia, kde je uvedený príklad ako sa používa protokol L2TP na pripojenie k IBM (R), cez Universal Connection.

Preklad sieťových adries pre VPN

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. Napríklad budete chcieť komunikovať s inou sieťou, ale obe siete používajú adresy 10.*.*.*, čo spôsobuje konflikt adries a vynechávanie celých 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 súčasnosti nepodporuje VPN NAT.

Ako by som mal používať 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.*.*.*. TO, ako nakonfigurujete tento typ VPN NAT závisí od toho, či váš server je iniciátor alebo respondent pre pripojenie VPN. Keď je váš server iniciátorom, môžete prekladať svoje lokálne adresy na také, ktoré sú kompatibilné s adresou pripojenia VPN vášho partnera. Keď je váš server respondentom, môžete prekladať vzdialené adresy VPN vášho partnera na také, ktoré sú kompatibilné s vašou lokálnou schémou adresovania. Tento typ prekladu adries nakonfigurujte len pre svoje dynamické pripojenia.

VPN NAT na skrývanie 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 server pre tieto pripojenia pracoval ako respondent.

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

1. Máte jeden alebo viac serverov, na ktoré chcete, aby ľudia pristupovali pomocou VPN?
2. Potrebujete byť flexibilní čo sa týka aktuálnych adries IP vášho systému?
3. Máte jednu alebo viac globálne smerovateľných adries IP?

Scenár *Použiť preklad sieťovej adresy pre VPN* uvádza príklad konfigurácie VPN NAT na skrytie lokálnych adries na vašom iSeries(TM).

Podrobný návod na nastavenie VPN NAT na iSeries nájdete v online pomoci dostupnej z rozhrania VPN v aplikácii iSeries Navigator.

IPSec kompatibilný s NAT

Problém: Bežný NAT prerušil 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.

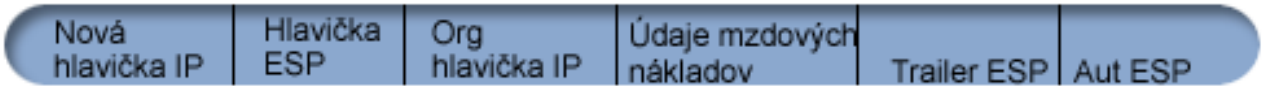
Riešenie: Zapuzdrenie UDP
Jedným slovom, zapuzdrenie UDP zabalí paket IPSec do novej, ale duplicitnej hlavičky IP/UDP. Adresa v novej hlavičke IP sa preloží, keď prechádza zariadením NAT. Potom ako paket dorazí na miesto určenia, prijímajúca strana zruší dodatočnú hlavičku a ponechá originálny paket 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 vo verzii v5r2 môže iSeries(TM) server fungovať ako klient pre zapuzdrenie UDP. Teda môže len *zahajovať* zapuzdrený prenos UDP.

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

Pôvodný datagram IPv4:

Po použití IPSec ESP v tunelovom režime:

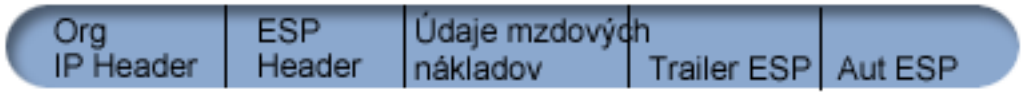


Po použití zapuzdrenia UDP:

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

Pôvodný datagram IPv4:

Po použití IPSec ESP v prenosovom režime:



Po použití zapuzdrenia UDP:

Po zapuzdrení paketu ho iSeries odošle jeho VPN partnerovi cez UDP, port 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. Preto, aby fungoval správne musia obidva konce pripojenia podporovať zapuzdrenie UDP.

Komprimácia IP (IPComp)

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)*. Túto RFC nájdete na Internete na nasledujúcej webovej stránke: http://www.rfc-editor.org.

Filtrovanie VPN a IP

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.

Od operačného systému V5R1 môže VPN generovať tieto pravidlá automaticky. Kedykoľvek je to možné, povoľte VPN, aby vám generovala filtre politík. Toto pomôže pri eliminácii chýb a zabezpečí, že pravidlá nebudete musieť konfigurovať oddelene použitím editora pravidiel pre pakety v aplikácii iSeries(TM) Navigator.

Existujú samozrejme výnimky. Prezrite si tieto témy a dozviete sa viac o ostatných, menej používaných konceptoch a technológiách filtrovania VPN, ktoré by sa mohli použiť vo vašej konkrétnej situácii:

- **Migrovať filtre politiky na aktuálne vydanie**
  Vo verziách V4R4 a V4R5 operačného systému musíte nakonfigurovať pravidlá pre pakety VPN ako samostatný

krok. Tieto neboli vygenerované automaticky ako súčasť vašich konfigurácií VPN. Táto téma podrobne popisuje špeciálne hľadiská pre migráciu filtrov politiky V4R4 a V4R5 na aktuálne vydanie a vyloží vám, ako ju vykonať.

- **Pripojenie 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. Táto téma vysvetľuje, prečo by ste to mali vziať do úvahy a načrtne postup.
- **Implicitná IKE**
  Aby sa pre vašu VPN vykonali vyjednávania IKE, musíte povoliť datagramy UDP cez port 500 pre tento typ prenosu IP. Ale ak nie sú na systéme žiadne pravidlá pre filtre konkrétne napísané na povolenie prenosu IKE, systém implicitne povolí tok prenosu IKE. V tejto téme nájdete viac informácií o fungovaní na iSeries.

Migrovať filtre politiky na aktuálne vydanie

V operačných systémoch V4R4 a V4R5 ste museli nakonfigurovať pravidlá pre pakety VPN samostatne v rozhraní pravidiel pre pakety aplikácie iSeries(TM) Navigator. Tieto neboli vygenerované automaticky ako súčasť vašich konfigurácií VPN. Od V5R1 operačného systému vie GUI VPN vytvárať tieto pakety automaticky.

Je niekoľko položiek, ktoré potrebujete vziať do úvahy, ak ste vo V4R4 alebo V4R5 vytvorili pravidlá pre filtre (pravidlá, kde action=IPSEC), a tie isté pravidlá chcete používať s aktuálnym vydaním. Alebo snáď VPN *vygeneruje* vaše pravidlá pre filtre politiky, ale musíte pridať dodatočné pravidlá, ktoré cez pripojenie povolia iný prenos IP, napríklad telnet. Postupujte podľa týchto odporúčaní, ktoré vám pomôžu vyhnúť sa potenciálnym chybám v konfigurácii.

Na objasnenie: Keď sa táto téma odvoláva na súbor s pravidlami pre *zákazníka*, odkazuje na každý súbor s pravidlami, ktorý ste vytvorili pomocou editora pravidiel pre pakety v aplikácii iSeries Navigator. Porovnajte to so súborom s pravidlami *VPNPOLICYFILTERS.I3P*, čo je súbor s pravidlami, ktorý VPN automaticky generuje ako súčasť konfigurácií VPN.

- Ak máte pripojenia VPN z V4R4 alebo V4R5 a neplánujete v aktuálnom vydaní konfigurovať iné pripojenia VPN, môžete zvyčajným spôsobom aktivovať svoje pravidlá pre filtre a spustiť pripojenia.
- Ak máte pripojenia VPN z verzie V4R4 alebo V4R5 a chcete nakonfigurovať nové pripojenie VPN v aktuálnom vydaní, použite sprievodcu **Migrovať filtre politiky**. Tento sprievodca odstráni filtre politiky zo súborov s pravidlami pre pakety, ktoré ste vytvorili a do VPNPOLICYFILTERS.I3P, ktorého generuje VPN, vloží ekvivalentné filtre politiky. Pre prístup k sprievodcovi postupujte podľa týchto krokov:
  1. V aplikácii iSeries Navigator rozviňte váš server **—> Sieť—> Politiky IP**.
  2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Migrovať filtre politiky**.
  3. Keď dokončíte sprievodcu, kliknite na **Dokončiť**.
  4. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
- Ak VPN vygenerovala vaše pravidlá pre filtre politiky, ale potrebujete pridať nejaké pravidlá pre filtre iné ako VPN, musíte nakonfigurovať tieto pravidlá pomocou editora pravidiel pre pakety v aplikácii iSeries Navigator. Ak niektoré z týchto pravidiel pre filtre iných ako VPN musia byť pred pravidlami pre filtre VPN, ich názvy množín začnite s PREIPSEC. Napríklad PREIPSECMYRULES. Toto pomáha systému zistiť poradie spracovania vašich filtrovacích pravidiel. Skupina názvov všetkých ostatných nie-VPN pravidiel nemôže mať prefix PREIPSEC. Napríklad MORERULES.
- Vždy umožnite VPN vytvárať filtrovacie pravidlá politiky. Ale vaše pravidlá iné ako VPN musia zostať vo vašom súbore s pravidlami pre zákazníkov. Nezabudnite, ak niektorý z týchto filtrov iných ako VPN musí byť pred filtrami politiky v súbore s pravidlami VPNPOLICYFILTERS.I3P, musíte na začiatok názvu množiny pridať PREIPSEC. Takto zaistíte, že vaše pravidlá pre zákazníkov a pravidlá VPN budú fungovať súčasne, ako ste mali v úmysle. Napríklad VPN vygenerovala vaše pravidlá pre filtre politiky (množiny VPN), ale vy ste pridali ďalšie pravidlá (vaše množiny), aby bola cez pripojenie umožnená aj iný prenos IP. Keď zavediete pravidlá do vášho systému, budú usporiadané nasledovne:
  1. Vaše množiny, ktorých názvy začínajú s PREIPSEC
  2. Množiny VPN, ktorých názov začína s PREIPSEC
  3. Množiny VPN s ACTION=IPSEC (filtre politiky)
  4. Vaše množiny s ACTION=IPSEC (filtre politiky)

5. Vaše množiny s čímkoľvek iným.
6. Množiny VPN s čímkoľvek iným.

Skontrolujte súbor EXPANDED.OUT, aby ste videli poradie pripojeného výstupného súboru. EXPANDED.OUT je zapísaný v adresári, v ktorom sa nachádza váš súbor s pravidlami pre zákazníkov.

- Použitím aplikácie iSeries Navigator si môžete vybrať aktiváciu:
  - len súboru s pravidlami, ktorý vygenerovala VPN, VPNPOLICYFILTERS.I3P
  - len vášho súboru s pravidlami pre zákazníkov
  - pravidiel vygenerovaných pomocou VPN a vášho súboru s pravidlami pre zákazníkov
- Aktivovať vaše pravidlá pre filtre na všetkých rozhraniach, namiesto podľa jednotlivých rozhraní. Toto pomáha zaručiť, že sa filtre aktivujú a tiež nastaviť správne poradie filtrov politiky.
- Pred pokusom o aktiváciu si vždy skontrolujte vaše filtrovacie pravidlá. Ak táto kontrola prebehne bez chýb, skontrolujte EXPANDED.OUT, aby ste sa uistili, že pravidlá sú zoradené v želanom poradí. Keď dokončíte tento krok, môžete aktivovať pravidlá.

Pripojenia VPN bez filtrov politiky

Pravidlo filtra politiky definuje, ktoré adresy, protokoly a porty, môžu používať VPN a nasmeruje príslušný prenos cez toto pripojenie. V niektorých prípadoch môžete nakonfigurovať pripojenie, ktoré nevyžaduje pravidlo pre filtre politiky. Napríklad máte na rozhraní zavedené pravidlá pre pakety iné ako VPN, ktoré bude vaše pripojenie VPN používať, takže namiesto deaktivácie aktívnych pravidiel na tomto rozhraní sa rozhodnete nakonfigurovať VPN tak, aby váš systém dynamicky riadil všetky filtre pre pripojenie. 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:

- Pripojenie môže zahájiť len lokálny server.
- 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

Ak chcete vytvoriť pripojenie, väčšina VPN vyžaduje dohodovanie IKE (Internet Key Exchange) pred tým, ako nastane spracovanie IPSec. 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.

Plán pre VPN

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**
  Skôr ako začnete sa uistite, že sú splnené všetky minimálne požiadavky pre vytvorenie VPN.
- **Zistiť, aký typ VPN vytvoriť**
  Zisťovanie toho, ako budete používať svoju VPN, je jedným z prvých krokov pri úspešnom plánovaní. Táto téma popisuje rôzne typy pripojenia, ktoré môžete nakonfigurovať.
- **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 Internet Key Exchange (IKE). Pre manuálne pripojenia pre vaše manuálne typy pripojenia použite plánovací pracovný hárok.

- **Vyplniť plánovacie pracovné hárky VPN**
  Ak to preferujete, plánovacie pracovné hárky VPN môžete vytlačiť a vyplniť na zozbieranie podrobných informácií o plánoch na používanie vašej VPN.

Po dokončení plánu pre vašu VPN môžete začať s jej konfiguráciou.

Požiadavky na nastavenie VPN

Pre správne fungovanie na iSeries(TM) a so sieťovými klientmi sa uistite, že váš počítač iSeries a vaše PC vyhovujú týmto požiadavkám:

Požiadavky na iSeries V5R2

- OS/400(R) verzia 5 vydanie 2 (5722-SS1) alebo novší
- Správca digitálnych certifikátov (5722-SS1 voľba 34)
- Poskytovateľ šifrovaného prístupu (5722-AC2 or AC3)
- iSeries Access for Windows(R)(5722-XE1) a iSeries Navigator
  - Komponent Sieť aplikácie iSeries 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(R), správne pripojeným k vášmu počítaču iSeries a nakonfigurovaný pre TCP/IP
- Ústredná jednotka 233 Mhz
- 32 MB RAM pre klientov Windows 95/98
- 64 MB RAM pre Windows NT(R) a klientov 2000
- Aplikácie iSeries Access for Windows a iSeries Navigator sú na klientskom PC nainštalované
- Softvér podporujúci protokol Bezpečnosť IP (IPSec)
- Softvér podporujúci L2TP, ak vzdialení užívatelia budú na vytvorenie pripojenia na váš systém používať L2TP

Zistiť, aký typ VPN vytvoriť

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 líšia sa koncové body *pripojenia* od koncových bodov *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.

Vyplniť plánovacie pracovné hárky VPN

Plánovacie pracovné hárky VPN môžete použiť na zozbieranie podrobných informácií o plánoch na používanie vašej VPN. Tieto informácie budete potrebovať na primerané naplánovanie stratégie vašej VPN. Tieto informácie môžete použiť aj na konfiguráciu vašej VPN. Zvoľte si pracovný hárok alebo typ pripojenia, ktorý chcete vytvoriť.

- **Plánovací pracovný hárok pre dynamické pripojenia**
  Vyplňte tento pracovný hárok predtým, ako nakonfigurujete dynamické pripojenie.
- **Plánovací pracovný hárok pre manuálne pripojenia**
  Vyplňte tento pracovný hárok predtým, ako nakonfigurujete manuálne pripojenie.
- **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 svoje dynamické pripojenia. Pre manuálne pripojenia pre vaše manuálne typy pripojenia použite plánovací pracovný hárok.

Ak vytvoríte viacero pripojení s podobnými vlastnosťami, môžete nastaviť predvolené hodnoty 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**.

Plánovací pracovný hárok pre dynamické pripojenia

Než vytvoríte vaše dynamické pripojenia VPN, vyplňte tento pracovný hárok. Pracovný hárok predpokladá, že použijete Sprievodcu novým pripojením. Sprievodca umožňuje nastaviť VPN na základe vašich základných bezpečnostných požiadaviek. V niektorých prípadoch budete musieť vyladiť vlastnosti, ktoré tento sprievodca konfiguruje pre pripojenie. Napríklad sa rozhodnete, že budete vyžadovať žurnálovanie alebo že chcete, aby sa server VPN spúšťal pri každom spustení TCP/IP. 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.

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je váš OS/400(R) V5R2 (5722-SS1) alebo novší?	
Je nainštalovaná voľba Správca digitálnych certifikátov (5722-SS1 voľba 34)?	
Je nainštalovaný Poskytovateľ šifrovaného prístupu (5722-AC2 alebo AC3)?	
Je nainštalovaný iSeries(TM) Access(5722-XE1)?	
Je nainštalovaný iSeries Navigator?	

Kontrolný zoznam nevyhnutných požiadaviek	Odpovede
Je nainštalovaný vedľajší komponent Sieť aplikácie iSeries Navigator?	
Sú nainštalované pomocné programy pre pripojiteľnosť TCP/IP pre OS/400 (5722-TC1)?	
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	
Je na vašom iSeries nakonfigurovaný 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 IKE (UDP port 500), AH a ESP?	
Sú firewally nakonfigurované tak, aby povoľovali postupovanie IP?	

Na konfiguráciu dynamického pripojenia VPN budete potrebovať tieto informácie	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 • Vyvážiť bezpečnosť a výkon • 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 koncového bodu údajov?	
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 • Vyvážiť bezpečnosť a výkon • Najnižšia bezpečnosť a najvyšší výkon	

Plánovací pracovný hárok pre manuálne pripojenia

Vyplňte tento pracovný hárok, ktorý vám pomôže pri vytváraní vašich pripojení Virtuálnej súkromnej siete (VPN), ktoré nepoužívajú IKE na správu kľúčov.

Skôr ako budete v nastavovaní VPN pokračovať, odpovedzte na každú z týchto otázok:

Kontrolný zoznam predbežných podmienok	Odpovede
Je váš systém OS/400(R) V5R2 (5722-SS1) alebo novší?	
Je nainštalovaná voľba Správca digitálnych certifikátov (5722-SS1 voľba 34)?	

Kontrolný zoznam predbežných podmienok	Odpovede
Je nainštalovaný Poskytovateľ šifrovaného prístupu (5722-AC2 alebo AC3)?	
Je nainštalovaný iSeries(TM) Access(5722-XE1)?	
Je nainštalovaný iSeries Navigator?	
Je nainštalovaný vedľajší komponent Sieť aplikácie iSeries Navigator?	
Sú nainštalované pomocné programy pre pripojiteľnosť TCP/IP pre OS/400 (5722-TC1)?	
Nastavili ste systémovú hodnotu bezpečnostných údajov zadržiavacieho servera (QRETSVRSEC *SEC) na 1?	
Je na vašom iSeries nakonfigurovaný 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?	

Na konfiguráciu manuálnej VPN budete potrebovať tieto informácie	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? Prečítajte 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)? Prečítajte si Bezpečnosť IP (IPSec), 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 svoj 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.	

Na konfiguráciu manuálnej VPN budete potrebovať tieto informácie	Odpovede
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.	
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.	

Nakonfigurovať VPN

Rozhranie VPN vám ponúka niekoľko rôznych spôsobov na konfiguráciu vašich pripojení VPN. Čítajte ďalej a ľahšie sa rozhodnete, ktorý typ pripojenia nakonfigurovať a ako postupovať.

Aký typ pripojenia by som mal nakonfigurovať?
Dynamické pripojenie je také, ktoré pomocou protokolu Internet Key Exchange (IKE) dynamicky generuje a vyjednáva kľúče, ktoré zabezpečujú vaše pripojenie, a súčasne je aktívne. 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 (stránka 36) pripojenie však neposkytuje podporu pre dohodovanie IKE a v dôsledku toho automatické riadenie 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 toto považujete za bezpečnostné riziko, môžete namiesto toho vytvoriť dynamické pripojenie.

Ako nakonfigurujem dynamické pripojenie VPN?
VPN je v skutočnosti skupina objektov konfigurácie, ktoré definuje charakteristiku pripojenia. Dynamické pripojenie VPN vyžaduje pre svoju správnu činnosť každý z týchto objektov. Nasledujte nasledujúce odkazy a získate špecifické informácie o tom, ako nakonfigurovať každý objekt konfigurácie VPN:

> **Návrh:**
> **Nakonfigurovať pripojenia so sprievodcom Nové pripojenie**
> Vo všeobecnosti môžete na vytvorenie všetkých vašich dynamických pripojení použiť sprievodcu pripojenia. Sprievodca automaticky vytvorí každý z objektov konfigurácie, ktoré VPN vyžaduje pre svoju správnu činnosť, vrátane pravidiel pre pakety. Ak zadáte, že chcete, aby sprievodca za vás aktivoval pravidlá VPN, môžete preskočiť na krok šesť, *Spustiť pripojenie*. V opačnom prípade, keď sprievodca skončí konfiguráciu vašej VPN, musíte aktivovať pravidlá pre pakety a potom budete môcť spustiť pripojenie.

Ak zvolíte nepoužiť sprievodcu na konfiguráciu vašich dynamických pripojení VPN, postupujte podľa týchto krokov a dokončíte konfiguráciu:

1. **Nakonfigurovať bezpečnostné politiky VPN**
   Musíte definovať bezpečnostné politiky VPN pre všetky vaše dynamické pripojenia. Politika Internet Key Exchange a údajová politika predpisujú, ako IKE ochraňuje svoje vyjednávania fázy 1 a fázy 2.

2. **Nakonfigurovať bezpečné pripojenia**
   Keď ste zadefinovali bezpečnostné politiky pre 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, zatiaľ čo **pripojenie dynamických kľúčov** definuje charakteristiky jednotlivých údajových pripojení medzi dvojicami koncových bodov. Pripojenie dynamických kľúčov existuje v skupine dynamických kľúčov.

   Poznámka: Ak vyberiete voľbu **Pravidlo pre pakety politiky bude definované v pravidlách pre pakety** na stránke **Skupina dynamických kľúčov - Pripojenia** v rozhraní VPN, musíte dokončiť len prvé dva kroky, *Nakonfigurovať pravidlá pre pakety* a *Definovať rozhranie pre pravidlá*. V opačnom prípade sa tieto pravidlá vytvoria ako súčasť vašich konfigurácií VPN a použijú sa na rozhranie, ktoré zadáte.

   Odporúča sa, aby ste vždy povolili rozhraniu VPN vytvoriť za vás vaše pravidlá pre filtre politiky. Za týmto účelom vyberte voľbu **Vygenerovať nasledujúci filter politiky pre túto skupinu** na stránke **Skupina dynamických kľúčov - Pripojenia**.
3. **Nakonfigurovať pravidlá pre pakety**
   Keď dokončíte vaše konfigurácie VPN, musíte vytvoriť a použiť pravidlá pre filtre, ktoré umožňujú údajom prenos cez pripojenie. Pravidlá VPN **pre-IPSec** umožňujú všetok prenos IKE na určených rozhraniach, takže IKE môže vyjednávať pripojenia. Pravidlo pre **filter politiky** definuje, ktoré adresy, protokoly a porty môže používať priradená nová skupina dynamických kľúčov.

   Ak prechádzate z verzie V4R4 alebo V4R5 a máte zadefinované pripojenia VPN a filtre politík, ktoré by ste chceli v aktuálnej verzii naďalej používať, pozrite si tému *Migrácia filtrov politík do aktuálneho vydania*, kde sa dozviete, či budú vaše staré a nové filtre politík spolu fungovať podľa vašich predstáv.
4. **Definovať rozhranie pre pravidlá**
   Keď ste nakonfigurovali pravidlá pre pakety a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré ich použiť.
5. **Aktivovať pravidlá pre pakety**
   Keď ste zadefinovali rozhranie pre vaše pravidlá pre pakety, musíte ich predtým, ako budete môcť spustiť pripojenie, aktivovať.
6. **Spustiť pripojenie**
   Pomocou tejto úlohy spustíte svoje pripojenie.

Ako nakonfigurujem manuálne pripojenie VPN?
Ako už naznačuje názov, manuálne pripojenie je také, kde všetky vlastnosti vášho VPN musíte nakonfigurovať ručne, vrátane vstupných a výstupných kľúčov. Konkrétne informácie o konfigurácii manuálneho pripojenia nájdete v nasledujúcom postupe:

1. **Nakonfigurovať manuálne pripojenia**
   Manuálne pripojenia definujú charakteristiky pripojenia vrátane voľby bezpečnostných protokolov a koncových bodov pripojenia a údajov.

   Poznámka: Ak vyberiete voľbu **Pravidlo pre pakety politiky bude definované v pravidlách pre pakety** na stránke **Manuálne pripojenie - Pripojenie** v rozhraní VPN, musíte dokončiť len prvé dva kroky, *Nakonfigurovať pravidlo pre pakety politiky* a *Definovať rozhranie pre pravidlá*. V opačnom prípade sa tieto pravidlá vytvoria ako súčasť vašich konfigurácií VPN.

   Odporúča sa, aby ste vždy povolili rozhraniu VPN vytvoriť za vás vaše pravidlá pre filtre politiky. Za týmto účelom vyberte voľbu **Vygenerovať filter politiky, ktorý sa zhoduje s koncovými bodmi údajov** na stránke **Manuálne pripojenie - Pripojenie**.
2. **Nakonfigurovať pravidlo pre filtre politiky**
   Keď nakonfigurujete atribúty manuálneho pripojenia, musíte vytvoriť a použiť pravidlo pre filtre politiky, ktoré umožňuje údajom prenos cez pripojenie. Pravidlo pre **filter politiky** definuje, ktoré adresy, protokoly a porty môže používať priradené pripojenie.
3. **Definovať rozhranie pre pravidlá**
   Keď ste nakonfigurovali pravidlá pre pakety a všetky ďalšie pravidlá, ktoré potrebujete na povolenie vášho pripojenia VPN, musíte definovať rozhranie, na ktoré ich použiť.

4. **Aktivovať pravidlá pre pakety**
   Keď ste zadefinovali rozhranie pre vaše pravidlá pre pakety, musíte ich predtým, ako budete môcť spustiť pripojenie, aktivovať.
5. **Spustiť pripojenie**
   Pomocou tejto úlohy spustíte pripojenia, ktoré sa inicializujú lokálne.

Nakonfigurovať pripojenia VPN so sprievodcom 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. Ale ak potrebujete do vášho VPN pridať funkciu, napríklad žurnálovanie alebo preklad sieťových adries pre VPN (VPN NAT), môžete ďalej vylepšiť svoju VPN pomocou hárkov vlastností príslušnej skupiny alebo pripojenia dynamických kľúčov. Za týmto účelom musíte najskôr zastaviť pripojenie, ak je aktívne. Potom kliknite pravým tlačidlom na skupinu alebo pripojenie dynamických kľúčov a vyberte **Vlastnosti**.

Kým začnete, dokončite Plánovacieho poradcu 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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
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**.

Nakonfigurovať bezpečnostné politiky VPN

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

- **Nakonfigurovať politiku Internet Key Exchange (IKE)**
  Politika IKE definuje, akú úroveň ochrany autentifikácie a šifrovania používa IKE počas vyjednávaní fázy 1. 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.
- **Nakonfigurovať údajovú politiku**
  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.

Keď nakonfigurujete vaše bezpečnostné politiky VPN, musíte potom nakonfigurovať bezpečné pripojenia.

Nakonfigurovať politiku Internet Key Exchange (IKE)

Politika IKE definuje, akú úroveň ochrany autentifikácie alebo šifrovania používa IKE počas vyjednávaní fázy 1. Fáza 1 IKE vytvorí kľúče, ktoré chránia správy, ktoré sa prenášajú v nasledujúcich vyjednávaniach fázy 2. VPN používa na autentifikáciu vyjednávaní fázy 1 buď podpisový režim RSA alebo dopredu zdieľané kľúče. Ak plánujete na autentifikáciu serverov kľúčov používať digitálne certifikáty, musíte ich najskôr nakonfigurovať pomocou Správcu digitálnych certifikátov (5722-SS1 Voľba 34). 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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečnostné politiky IP**.

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. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Kliknite na **OK** a vaše zmeny sa uložia.

Poznámka: Vždy, keď je na autentifikáciu použitý dopredu zdieľaný kľúč, odporúča sa 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. Podrobnejšie informácie nájdete v online pomoci aplikácie iSeries Navigator.

Nakonfigurovať údajovú politiku

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).

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečnostné politiky IP**.
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. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Kliknite na **OK** a vaše zmeny sa uložia.

Nakonfigurovať bezpečné pripojenie 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 nakonfigurovať objekt bezpečnostného pripojenia, vykonajte nasledovné úlohy:

Časť 1: Nakonfigurujte skupinu dynamických kľúčov:

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**.
2. Kliknite pravým tlačidlom na **Podľa skupiny** a vyberte **Nová skupina dynamických kľúčov**.
3. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Kliknite na **OK** a vaše zmeny sa uložia.

Časť 2: Nakonfigurujte pripojenie dynamických kľúčov:

1. V aplikácii iSeries Navigator rozviňte váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia—> Podľa skupiny**.
2. V ľavej časti okna aplikácie iSeries Navigator kliknite pravým tlačidlom na skupinu dynamických kľúčov, ktorú ste vytvorili v časti jedna a vyberte **Nové pripojenie dynamických kľúčov**.
3. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Kliknite na **OK** a vaše zmeny sa uložia.

Keď dokončíte tieto kroky musíte aktivovať pravidlá pre pakety, ktoré toto pripojenie vyžaduje pre svoju správnu činnosť.

Poznámka: Vo väčšine prípadov povoľte rozhraniu VPN automaticky generovať vaše pravidlá pre pakety VPN výberom voľby **Generovať nasledujúci filter politiky pre túto skupinu** na stránke **Skupina dynamických kľúčov - Pripojenia**. Ale ak vyberiete voľbu **Pravidlá pre filtre politiky sa budú definovať v pravidlách pre pakety**, musíte nakonfigurovať pravidlá pre pakety VPN pomocou editora pravidiel pre pakety a potom ich aktivovať.

Nakonfigurovať manuálne pripojenie

Ako už naznačuje názov, manuálne pripojenie je také, kde všetky vlastnosti vášho VPN musíte nakonfigurovať ručne. 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 toto považujete za bezpečnostné riziko a oba konce pripojenia podporujú protokol Internet Key Exchange (IKE), môžete namiesto toho nastaviť dynamické pripojenie.

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**.
2. Kliknite pravým tlačidlom na **Všetky pripojenia** a vyberte **Nové manuálne pripojenie**.
3. Vyplňte všetky hárky vlastností. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Kliknite na **OK** a vaše zmeny sa uložia.

Poznámka: vo väčšine prípadov umožňuje rozhranie VPN automaticky generovať pravidlá pre pakety VPN výberom voľby **Generovať filter politiky zhodujúci sa s bodmi ukončenia** na stránke **Manuálne pripojenie - Pripojenie**. Ale ak vyberiete voľbu **Pravidlá pre filtre politiky sa budú definovať v pravidlách pre pakety**, musíte nakonfigurovať pravidlá pre filtre politiky ručne a potom ich aktivovať.

Nakonfigurovať pravidlá pre pakety

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 sa rozhodnete vytvoriť pravidlá pre pakety VPN použitím editora pravidiel pre pakety, v aplikácii iSeries(TM) Navigator, vytvorte všetky dodatočné pravidlá touto istou cestou. 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 nasledujúcu tému, kde sa dozviete, ako konfigurovať tieto pravidlá pomocou editora pravidiel pre pakety v aplikácii iSeries Navigator. Ak si želáte zobraziť informácie o ďalších možnostiach pre VPN a filtrovanie pozrite si časť *Filtrovanie VPN a IP* témy Koncepty VPN.

- **Pravidlá 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. Možno budete potrebovať pridať iné pravidlá pre-IPSec v závislosti od vášho príslušného sieťového prostredia a bezpečnostnej politiky.

  Poznámka: Potrebujete nakonfigurovať len tento typ pravidla pre-IPSec, ak už máte iné pravidlá, ktoré povoľujú IKE pre špecifické systémy. Ak nie sú na systéme napísané žiadne filtrovacie pravidlá na povolenie prenosu IKE, potom je prenos IKE implicitne povolený.
- **Pravidlá pre filtre politiky**
  Pravidlo pre filtre politiky definuje prenos, ktorý môže používať VPN a aká politika ochrany údajov sa má použiť na tento prenos.

Záležitosti, ktoré treba vziať do úvahy predtým, ako začnete
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 možno zistíte, že prenos, ktorý predtým fungoval, záhadne zlyhá, keď aktivujete vaše pravidlá pre filtre VPN. Ak chcete na rozhraní povoliť iný prenos ako VPN, musíte pridať výslovné pravidlá PERMIT.

Keď nakonfigurujete príslušné pravidlá pre filtre, musíte definovať rozhranie, na ktoré sa použijú a potom ich aktivovať.

Je nevyhnutné, aby ste svoje pravidlá pre filtre správne nakonfigurovali. V opačnom prípade pravidlá pre filtre môžu zablokovať všetok prenos IP prichádzajúci na a odchádzajúci z vášho iSeries. Platí to aj pre vaše pripojenie na aplikáciu iSeries Navigator, ktorú používate na konfiguráciu pravidiel pre filtre.

Ak pravidlá pre filtre nepovoľujú prenos pre aplikáciu iSeries Navigator, navigátor nebude môcť komunikovať s vašim iSeries. Ak je toto váš prípad, musíte sa prihlásiť na váš počítač iSeries použitím rozhrania, ktoré je stále pripojené, ako napríklad operačná konzola. 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.

Konfigurácia pravidiel pre filtre pre-IPSec

Upozornenie: Takto postupujte iba v prípade, keď ste zadali, že si neprajete aby VPN automaticky generovala vaše filtrovacie pravidlá politík.

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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Otvorí sa editor pravidiel pre pakety, ktorý vám umožní vytvoriť alebo upraviť filter a pravidlá NAT pre váš iSeries.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore pravidiel pre pakety vyberte **Vložiť —> 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 ľahšia voľba na povolenie prenosu IKE cez pripojenie je nakonfigurovať len filter pre-IPSec a v poliach **Smer**, **Názov zdrojovej adresy** a **Názov cieľovej adresy** použiť hodnoty s náhradnými znakmi (*).

Ďalším krokom je nakonfigurovať pravidlá pre filtre politiky na definovanie, aký prenos IP ochraňuje pripojenie VPN.

Nakonfigurovať pravidlo pre filtre politiky

Upozornenie: Takto postupujte iba v prípade, keď ste zadali, že si neprajete aby VPN automaticky generovala vaše filtrovacie pravidlo 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-IPSec, (pre dynamické pripojenia) editor pravidiel pre pakety bude stále otvorený; prejdite na krok 4.

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Otvorí sa editor pravidiel pre pakety, ktorý vám umožní vytvoriť alebo upraviť filter a pravidlá NAT pre váš iSeries.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore pravidiel pre pakety vyberte **Vložiť —> 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. Keď ich definujete pomocou funkcie **Definovať adresy**, môžete zadať aj rozsah adries IP alebo adresu IP plus masku podsiete.
8. Pre **Názov cieľovej adresy** v prvom poli vyberte **=** a v druhom poli zadajte adresu IP vzdialeného koncového bodu údajov. Keď ich definujete pomocou funkcie **Definovať adresy**, môžete zadať aj rozsah adries IP alebo adresu IP plus masku podsiete.

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 Port zdroja** a **Port cieľa** vyberte príslušnú hodnotu pre prenos. Alebo z rozbaľovacieho zoznamu môžete vybrať hviezdičku (*). Takto ktorémukoľvek protokolu používajúcemu ktorýkoľvek port povolíte používať VPN.
14. Kliknite na **OK**.

Ďalším krokom je definovať rozhranie, na ktoré sa tieto pravidlá pre filtre použijú.

Poznámka: Keď pridáte pravidlá pre filtre pre rozhranie, 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 možno zistíte, že pripojenia, ktoré predtým fungovali, záhadne zlyhajú, keď aktivujete vaše pravidlá pre pakety VPN. Ak chcete na rozhraní povoliť iný prenos ako VPN, musíte pridať výslovné pravidlá PERMIT.

Definovať rozhranie pre pravidlá pre filtre 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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Pravidlá pre pakety** a vyberte **Editor pravidiel**. Otvorí sa editor pravidiel pre pakety, ktorý vám umožní vytvoriť alebo upraviť filter a pravidlá NAT pre váš iSeries.
3. V privítacom okne vyberte **Vytvoriť nový súbor pravidiel pre pakety** a kliknite na **OK**.
4. V editore pravidiel pre pakety vyberte **Vložiť —> Rozhranie filtra**.
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 sa uloží do integrovaného súborového systému na vašom iSeries s príponou .i3p.
   Poznámka: Neukladajte váš súbor do nasledujúceho 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.

Keď ste zadefinovali rozhranie pre vaše pravidlá pre filtre, musíte ich predtým, ako budete môcť spustiť VPN, aktivovať.

Aktivovať pravidlá 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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
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.

Ak Po aktivácii pravidiel pre filtre môžete spustiť pripojenie VPN.

Spustiť pripojenie VPN

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
2. Ak nie je server VPN spustený, kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Spustiť**. Takto spustíte server VPN.
3. Skontrolujte, či sú vaše pravidlá pre pakety aktivované.
4. Rozviňte **Virtuálne súkromné siete—> 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**.

Riadiť VPN

Použite rozhranie VPN v aplikácii iSeries(TM) Navigator na spracovanie všetkých vašich riadiacich úloh, ktoré zahŕňajú:

- **Spustiť pripojenie VPN**
  Pomocou tejto úlohy spustíte pripojenia, ktoré sa zahajujú lokálne.
- **Nastaviť predvolené atribúty pre vaše 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.
- **Resetovať pripojenia v chybovom stave**
  Resetovanie chybných pripojení ich navráti do stavu nečinnosti.
- **Zobraziť informácie o chybách**
  Vykonajte túto úlohu, ktorá vám pomôže zistiť, prečo je vaše pripojenie chybné.
- **Zobraziť atribúty aktívnych pripojení**
  Vykonajte túto úlohu na kontrolu stavu a iných atribútov vašich aktívnych pripojení.
- **Použiť sledovanie servera VPN**
  Sledovanie servera VPN umožňuje konfigurovať, spúšťať, zastavovať a zobrazovať 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.

- **Zobraziť protokoly úloh servera VPN**
  Podľa týchto inštrukcií zobrazíte protokoly úloh pre Správcu kľúčov VPN a Správcu pripojení VPN.
- **Zastaviť pripojenia**
  Pomocou tejto úlohy zastavíte aktívne pripojenia.
- **Zobraziť atribúty bezpečnostných asociácií (Security Associations, SA)**
  Pomocou tejto úlohy zobrazíte atribúty Bezpečnostných asociácií (SA), ktoré sú priradené k povolenému pripojeniu.
- **Vymazať objekty konfigurácie VPN**
  Než vymažete objekt konfigurácie VPN z databázy politík VPN, uistite sa, či rozumiete tomu, ako to ovplyvní ostatné pripojenia a skupiny pripojení VPN.

Nastaviť predvolené atribúty pre vaše pripojenia

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 aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete** a vyberte **Predvolené hodnoty**.
3. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
4. Keď ste dokončili všetky hárky s vlastnosťami, kliknite na **OK** .

Resetovať pripojenia v chybovom stave

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**
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**.

Zobraziť informácie o chybách

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**
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**.

Zobraziť atribúty aktívnych pripojení

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Kliknite pravým tlačidlom na aktívne pripojenie alebo pripojenie na požiadanie, ktoré chcete zobraziť a vyberte **Vlastnosti**
4. Prejdite na stránku **Aktuálne atribúty** a uvidíte atribúty pripojenia.

Z okna aplikácie iSeries Navigator môžete zobraziť aj atribúty všetkých pripojení. 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 aplikácii iSeries Navigator rozviňte váš server —> **Sieť**—> **Politiky IP**—> **Virtuálne súkromné siete**—> **Bezpečné pripojenia**
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.
3. Z ponuky **Objekty** vyberte **Stĺpce**. Otvorí sa dialógové okno, v ktorom môžete vybrať atribúty, ktoré chcete zobraziť v okne iSeries Navigator.

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

Použiť sledovanie servera VPN

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server —> **Sieť**—> **Politiky IP**.
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete**, 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 stránke **Správca kľúčov** zadajte, aký typ sledovania chcete, aby server Správcu kľúčov spustil.
4. Ak máte otázky o tom, ako vyplniť stránku alebo niektoré z jej polí, kliknite na **Pomoc**.
5. Kliknite na **OK** a vaše zmeny sa uložia.
6. Kliknutím na

   Ikona pre Štart (Štart) spustíte sledovanie. Pravidelným klikaním na

   ″Ikona pre Obnoviť″ > (Obnoviť) zobrazíte najnovšie informácie o sledovaní.

Zobraziť protokoly úloh servera VPN

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server —> **Sieť**—> **Politiky IP.**
2. Kliknite pravým tlačidlom na **Virtuálne súkromné siete**, vyberte **Diagnostické nástroje** a potom vyberte ktorýkoľvek protokol úloh servera, ktorý chcete zobraziť.

Zobraziť atribúty bezpečnostných asociácií (Security Associations, SA)

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server —> **Sieť**—> **Politiky IP**—> **Virtuálne súkromné siete**—> **Bezpečné pripojenia**
2. Kliknite na **Všetky pripojenia** a v pravom okne sa zobrazí zoznam pripojení.

3. Kliknite pravým tlačidlom na príslušné aktívne pripojenie a vyberte **Bezpečnostné asociácie.**Výsledné okno umožní zobraziť vlastnosti každého SA priradeného k špecifickému pripojeniu.

Zastaviť pripojenie VPN

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**
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**.

Vymazať objekty konfigurácie VPN

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

1. V aplikácii iSeries(TM) Navigator rozviňte pre váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia**
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

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 túto zložitosť môžete so svojimi pripojeniami VPN občas zažiť nejaké ťažkosti. 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. Nasledujúce témy ponúkajú rady, ako odstrániť rôzne problémy, s ktorými sa môžete stretnúť pri používaní VPN:

- **Začíname s odstraňovaním problémov s VPN**
  Tu začnite s vyhľadávaním a opravou problémov s pripojením vašej VPN.
- **Bežné chyby konfigurácie VPN a ako ich opravovať**
  Táto téma identifikuje najbežnejšie užívateľské chyby a poskytuje možné riešenia.
- **Odstraňovanie problémov s VPN so žurnálom QIPFILTER**
  Táto téma poskytuje informácie o vašich pravidlách pre filtre VPN.
- **Odstraňovanie problémov s VPN so žurnálom QVPN**
  Táto téma poskytuje informácie o prenose a pripojeniach IP.
- **Odstraňovanie problémov VPN s protokolmi úloh VPN**
  Táto téma popisuje rôzne protokoly úloh, ktoré VPN používa.
- O**dstraňovanie problémov VPN s OS/400(R) Communications trace**
  Táto téma popisuje, ako sledovať údaje na komunikačnej linke.

Začíname s odstraňovaním problémov s VPN

Existuje niekoľko spôsobov, ako začať analýzu problémov s VPN:

1. Vždy sa presvedčte, či ste použili najnovšie dočasné opravy programu (PTF).
2. Presvedčte sa, či spĺňate minimálne požiadavky na nastavenie VPN.
3. Prezrite všetky chybové správy nachádzajúce sa v okne Informácie o chybách alebo Protokoly úloh servera VPN pre lokálne aj vzdialené systémy. 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 objavené chybové správy neposkytujú dostatok informácií na vyriešenie problému, skontrolujte žurnál Filter IP.

5. Sledovanie komunikácie na iSeries(TM) vám poskytuje ďalšie miesto na nájdenie všeobecných informácií o tom, či lokálny systém prijíma alebo odosiela požiadavky na pripojenie.
6. Príkaz Trace TCP Application (TRCTCPAPP) poskytuje ešte iný spôsob na izoláciu problémov. Zvyčajne IBM(R) Service používa TRCTCPAPP na získanie výsledku sledovania za účelom analýzy problémov s pripojením.

Ktoré veci ešte treba skontrolovať
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: Nezabudnite reagovať na výzvu príkazu PING; zadajte adresu vzdialeného systému a pre dodatočné parametre použite PF10, a potom zadajte lokálnu IP adresu. 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: Môžu existovať prostredné smerovače alebo firewall, ktoré vykonávajú filtrovanie paketov IP a môžu 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. Môžete vyskúšať iné protokoly IP na overenie pripojiteľnosti medzi dvomi systémami, napríklad Telnet a FTP.
2. Skontrolujte pravidlá pre filtre pre VPN a presvedčte sa, či sú aktivované. Spustilo sa filtrovanie úspešne? Ak odpoviete **áno**, prejdite ku kroku 3. Ak odpoviete **nie**, skontrolujte chybové správy v okne Pravidlá pre pakety v aplikácii iSeries 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

Táto časť popisuje niektoré z bežnejších problémov, ktoré sa vyskytujú s VPN a spojí vás s odporúčaniami, ako ich vyriešiť.

Poznámka: Keď konfigurujete VPN, v skutočnosti vytvárate niekoľko rôznych konfiguračných objektov, ku ktorým VPN vyžaduje povoliť 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.

Bežné chybové správy, s ktorými sa môžete stretnúť

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

Položka sa nenašla	Keď kliknete pravým tlačidlom na objekt VPN a vyberiete **Vlastnosti** alebo **Vymazať**, dostanete správu, ktorá uvádza **Položka sa nenašla**.
PARAMETER PINBUF JE NEPLATNÝ	Keď sa pokúsite spustiť pripojenie, dostanete správu, ktorá uvádza **PARAMETER PINBUF JE NEPLATNÝ...**
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.
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.
Nedá sa zašifrovať kľúč...	Dostanete správu, ktorá oznámi, že systém nemôže zašifrovať vaše kľúče, lebo hodnota QRETSVRSEC musí byť nastavená na 1.
CPF9821	Pri pokuse o rozvinutie alebo otvorenie kontajnera IP politík v aplikácii iSeries(TM) Navigator sa objaví správa CPF9821-Neautorizovaný do programu QTFRPRS v knižnici QSYS.

Iné problémy, do ktorých sa môžete dostať

Chyba	**Symptóm**
Všetky kľúče sú prázdne	Keď zobrazíte vlastnosti manuálneho pripojenia, všetky dopredu zdieľané kľúče a kľúče algoritmu pre pripojenie sú prázdne.
Objaví sa prihlásenie do iného systému	Keď v aplikácii iSeries Navigator prvýkrát použijete rozhranie pravidiel pre pakety, zobrazí sa prihlásenie do iného systému, ako je aktuálny.
Žiadny stav pripojenia	V stĺpci **Stav** v okne aplikácie iSeries Navigator nemá pripojenie žiadnu hodnotu.
Zastavené pripojenia stále povolené	Keď zastavíte pripojenie, okno aplikácie iSeries Navigator označuje, že pripojenie je stále povolené.
3DES nie je voľba pre šifrovanie	Keď pracujete s premenou politiky IKE, premenou údajovej politiky alebo manuálnym pripojením, šifrovací algoritmus 3DES nie je voľbou.
Zobrazenie neočakávaných stĺpcov	Nastavili ste stĺpce, ktoré chcete zobraziť v okne aplikácie iSeries Navigator pre vaše pripojenia VPN. Potom, keď sa na ne pozriete neskôr, zobrazia sa iné stĺpce.
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.
Skupina dynamických kľúčov 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.

Chybová správa VPN: TCP5B28

Symptóm:
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

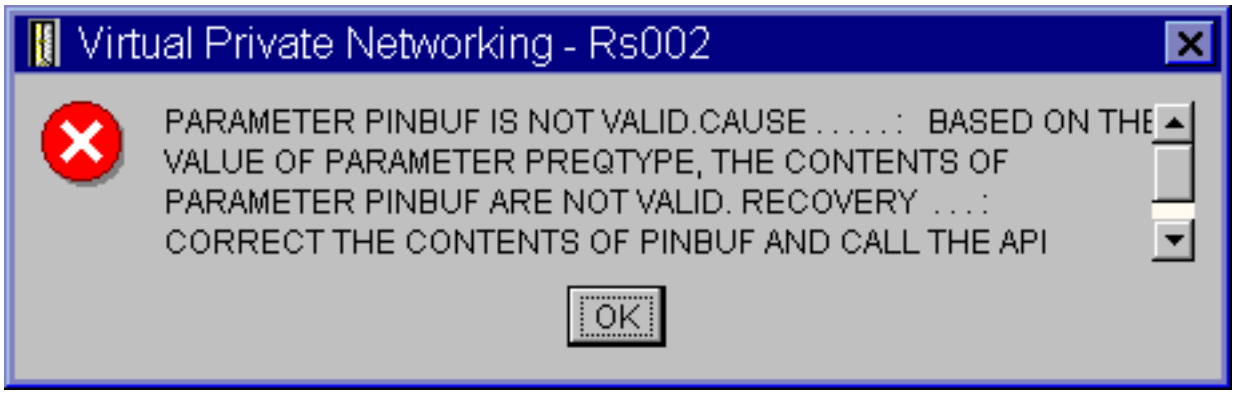
Symptóm:
Keď kliknete pravým tlačidlom na objekt v okne Virtuálne súkromné siete a vyberiete **Vlastnosti** alebo **Vymazať**, objaví sa nasledujúca správa:

Možné riešenie:

- Možno ste objekt vymazali alebo ho premenovali a ešte ste neobnovili 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.
- Pri konfigurácii vlastností objektu mohla nastať komunikačná chyba medzi serverom VPN a vašim iSeries(TM). Mnohé z objektov, ktoré sa zobrazujú v okne Virtuálne súkromné siete sa vzťahovali na viac ako jeden objekt v databáze politík VPN. To znamená, že komunikačné chyby mohli spôsobiť niektoré objekty v databáze, ktoré sa aj naďalej vzťahovali na 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

Symptóm:
Keď sa pokúsite spustiť pripojenie, objaví sa správa podobná nasledujúcej:



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...

Symptóm:
Keď vyberiete **Vlastnosti** pre pripojenie dynamických kľúčov, objaví sa správa podobná nasledujúcej:

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

Symptóm:
Keď na pracovnom hárku vlastností pre skupinu dynamických kľúčov alebo manuálne pripojenie vyberiete **OK**, objaví sa nasledujúca 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...

Symptóm:
Objaví sa nasledovná 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**.

Chybová správa VPN: CPF9821

Symptóm:
Pri pokuse o rozvinutie kontajnera IP politík sa v aplikácii iSeries(TM) Navigator zobrazí správa CPF9821 - Neautorizovaný do programu QTFRPRS v knižnici QSYS.

Možné riešenie:
Možno nemáte vyžadované oprávnenie na obnovu aktuálneho stavu Pravidiel pre pakety alebo Správcu pripojení VPN. Skontrolujte, či máte nastavené oprávnenia *IOSYSCFG na získanie prístupu k funkciám pravidiel pre pakety v aplikácii iSeries Navigator.

Chyba VPN: Všetky kľúče sú prázdne

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

Možné riešenie:
To sa stane vždy, keď sa hodnota QRETSVRSEC nastaví späť na 0. Nastavením tejto hodnoty na 0 sa vymažú všetky

kľúče v databáze politík VPN. Ak chcete opraviť tento problém, musíte nastaviť systémovú hodnotu na 1 a potom znova zadať všetky kľúče. Pozrite si tému Chybová správa: Nedajú sa zašifrovať kľúče, kde nájdete viac informácií o tom, ako to vykonať.

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

Symptóm:
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 aplikácii iSeries(TM) Access príslušnú konverznú tabuľku pre unicode. Toto nastane len jedenkrát.

Chyba VPN: Prázdny stav pripojenia v okne aplikácie iSeries Navigator

Symptóm:
Pripojenie nemá žiadnu hodnotu v stĺpci **Stav** v okne aplikácie iSeries(TM) 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

Symptóm:
Po ukončení pripojenia okno aplikácie iSeries(TM) Navigator zobrazuje, že pripojenie je stále aktívne.

Možné riešenie:
Toto sa stane, keď neaktualizujete okno aplikácie iSeries Navigator. To znamená, že obsahuje neaktuálne informácie. Ak to chcete napraviť, z ponuky **Zobrazenie** vyberte **Obnoviť**.

Chyba VPN: 3DES nie je voľba pre šifrovanie

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

Možné riešenie:
Najpravdepodobnejšie máte na svojom systéme nainštalovaný produkt Cryptographic Access Provider AC2 (5722-AC2) a nie Cryptographic Access Provider AC3 (5722-AC3). AC2 umožňuje len šifrovací algoritmus Data Encryption Standard (DES) vzhľadom na obmedzenia dĺžky kľúčov.

Chyba VPN: V okne aplikácie iSeries Navigator sa zobrazili neočakávané stĺpce

Symptóm:
Nastavili ste stĺpce, ktoré chcete zobraziť v okne aplikácie iSeries Navigator pre vaše pripojenia VPN. Potom, keď sa na ne pozriete neskôr, zobrazia sa iné 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

Symptóm:
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

Symptóm:
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 so žurnálom QIPFILTER

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.

Ako povoliť žurnál filtrovania paketov IP
Použite editor pravidiel pre pakety v aplikácii iSeries(TM) Navigator 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 aplikácii iSeries Navigator rozviňte váš server —> **Sieť**—> **Politiky IP**.
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.

Ako používať žurnál QIPFILTER
OS/400(R) pri prvej aktivácii filtrovania IP paketov automaticky vytvorí žurnál. 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 o povolení alebo zamietnutí pravidiel pre filtre, kde je voľba žurnálovania nastavená na hodnotu 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.

Prečítajte si žurnálové polia QIPFILTER, kde nájdete tabuľku popisujúcu výstupné súbory QIPFILTER.

Žurnálové súbory QIPFILTER

Nasledujúca tabuľka popisuje polia vo výstupnom súbore QIPFILTER:

Názov poľa	Dĺžka poľa	Numerické	Popis	Komentáre
TFENTL	5	Y	Dĺžka položky	
TFSEQN	10	Y	Sekvenčné číslo	
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

Názov poľa	Dĺžka poľa	Numerické	Popis	Komentáre
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*

Odstraňovanie problémov s VPN so žurnálom QVPN

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.

Ako povoliť žurnál VPN

Použite rozhranie virtuálnej súkromnej siete v aplikácii iSeries(TM) Navigator 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 aplikácii iSeries Navigator rozviňte váš server **—> Sieť—> Politiky IP—> Virtuálne súkromné siete—> Bezpečné pripojenia.**
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:
   Žiadne
   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.
Činnosť pripojenia
Žurnálovanie sa bude vykonávať pre také činnosti pripojenia, ako je spúšťanie alebo zastavovanie pripojenia.
Preprava 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: Kým budete môcť zastaviť žurnálovanie, uistite sa, že pripojenie je neaktívne. Ak chcete zmeniť stav skupiny pripojení, uistite sa, že s touto konkrétnou skupinou nie sú spojené žiadne aktívne pripojenia.

Ako používať žurnál VPN
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.

Prečítajte si žurnálové polia QVPN, kde nájdete tabuľku popisujúcu polia vo výstupnom súbore VPN.

Žurnálové súbory QVPN

Nasledujúca tabuľka 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	

Názov poľa	Dĺžka poľa	Numerické	Opis	Poznámka
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	
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	

Odstraňovanie problémov VPN s protokolmi 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.

Je dôležité, aby ste analyzovali protokoly úloh na oboch stranách pripojenia, ak sú obidve strany servery iSeries(TM). 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. Môžete si pozrieť ich vlastné protokoly úloh z aplikácie OS/400(R) iSeries 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. Súvisiaci 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.

Chybové správy Správcu pripojení VPN
Táto časť popisuje niektoré z bežnejších chybových správ Správcu pripojení VPN, ktoré môžete zaznamenať.

Správca pripojení VPN zaprotokoluje dve správy v protokole úloh QTOVMAN, keď sa vyskytne chyba pri pripojení VPN. Prvá správa poskytuje podrobnosti ohľadne chyby. Informácie o týchto chybách môžete vidieť v aplikácii iSeries(TM) Navigator, ak kliknete pravým tlačidlom myši na pripojenie a vyberiete **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	Obnovenie
TCP8601 Nedá sa spustiť pripojenie VPN [*názov pripojenia*]	Nedalo sa spustiť toto pripojenie VPN kvôli týmto kódom príčiny: *0* - Predchádzajúca správa v protokole úloh s rovnakým názvom pripojenia VPN obsahuje podrobnejšie 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. V protokole úloh vyhľadajte ďalšie správy. 2. Opravte chyby a skúste požiadavku znova. 3. Na zobrazenie stavu pripojenia použite iSeries Navigator. Pripojenia, ktoré sa nedali spustiť, budú v chybovom stave.

Správa	Príčina	Obnovenie
TCP8602 Vyskytla sa chyba pri zastavovaní pripojenia VPN [*názov pripojenia*]	Bolo vyžadované zastavenie určeného pripojenia VPN, ale nezastavilo sa alebo sa zastavilo s chybou následkom kódu príčiny: *0* - Predchádzajúca správa v protokole úloh s rovnakým názvom pripojenia VPN obsahuje podrobnejšie 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. V protokole úloh vyhľadajte ďalšie správy. 2. Opravte chyby a skúste požiadavku znova. 3. Na zobrazenie stavu pripojenia použite iSeries Navigator. Pripojenia, ktoré sa nedali spustiť, budú v chybovom stave.
TCP8604 Spustenie pripojenia VPN [*názov pripojenia*] zlyhalo	Spustenie tohto pripojenia VPN zlyhalo následkom týchto kódov príčiny: *1* - Nedal sa 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. V protokole úloh vyhľadajte ďalšie správy. 2. Opravte chyby a skúste požiadavku znova. 3. Na kontrolu alebo opravu konfigurácie politiky VPN použite aplikáciu iSeries Navigator. 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. V protokole úloh vyhľadajte ďalšie správy. 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 spôsobí, že sa ukončia všetky aktuálne pripojenia VPN.

Správa	Príčina	Obnovenie
TCP8606 Správa kľúčov VPN nemohol vytvoriť vyžadovanú bezpečnostnú asociáciu pre pripojenie [*názov pripojenia*]	Správa kľúčov VPN nemohol vytvoriť vyžadovanú bezpečnostnú asociáciu následkom jedného z týchto kódov príčiny: *24* - Autentifikácia pripojenia Správcu kľúčov VPN zlyhala. *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. V protokole úloh vyhľadajte ďalšie správy. 2. Opravte chyby a skúste požiadavku znova. 3. Na kontrolu alebo opravu konfigurácie politiky VPN použite aplikáciu iSeries Navigator. Skontrolujte, či skupina dynamických kľúčov priradené k tomuto pripojeniu má nakonfigurované prijateľné hodnoty.
TCP8608 Pripojenie VPN, [*Názov pripojenia*], nemohlo získať adresu NAT	Táto skupina dynamických kľúčov alebo toto údajové pripojenie určilo, že preklad sieťovej adresy (network address translation, NAT) je dokončený na jednej alebo viacerých adresách a že zlyhal následkom jedného z týchto kódov príčiny: *1* - Adresa, na ktorú sa má použiť NAT, nie je samostatná adresa IP. *2* - Všetky dostupné adresy sa už použili.	1. V protokole úloh vyhľadajte ďalšie správy. 2. Opravte chyby a skúste požiadavku znova. 3. Na kontrolu alebo opravu politiky VPN použite aplikáciu iSeries Navigator. Skontrolujte, či skupina dynamických kľúčov priradené k tomuto pripojeniu má nakonfigurované prijateľné hodnoty pre adresy.
TCP8620 Koncový bod lokálneho pripojenia nie je k dispozícii	Tieto pripojenia VPN sa nedali povoliť, lebo koncový bod lokálneho pripojenia nebol k dispozícii.	1. V protokole úloh vyhľadajte ďalšie správy patriace 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 nie je k dispozícii	Toto pripojenie VPN sa nedalo povoliť, lebo koncový bod lokálnych údajov nebol k dispozícii.	1. V protokole úloh vyhľadajte ďalšie správy patriace 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.

Správa	Príčina	Obnovenie
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. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zmenu politiky VPN spojenej s týmto pripojením použite aplikáciu iSeries Navigator. 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. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zobrazenie všetkých povolených pripojení, ktoré majú lokálne koncové body údajov a vzdialené koncové body údajov prekrývajúce pripojenie, použite aplikáciu iSeries Navigator. Ak sa vyžadujú oba pripojenia, zmeňte politiku existujúceho pripojenia. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8624 Pripojenie VPN nie je v rozsahu 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. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zobrazenie obmedzení pre koncový bod údajov pre toto pripojenie alebo skupinu dynamických kľúčov použite aplikáciu iSeries Navigator. 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 zlyhalo pri kontrole algoritmu ESP	Toto pripojenie VPN sa nedalo povoliť, lebo tajný kľúč priradený k pripojeniu bol nedostatočný.	1. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zobrazenie politiky priradenej k tomuto pripojeniu a na zadanie iného tajného kľúča použite aplikáciu iSeries Navigator. 3. Opravte všetky chyby a skúste požiadavku znova.

Správa	Príčina	Obnovenie
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. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zobrazenie obmedzení pre koncový bod údajov pre toto pripojenie alebo skupinu dynamických kľúčov použite aplikáciu iSeries Navigator. 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.
TCP8628 Pravidlo pre filtre politiky nie je zavedené	Pravidlo pre filtre politiky pre toto pripojenie nie je aktívne.	1. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zobrazenie filtrov aktívnej politiky použite aplikáciu iSeries Navigator. Skontrolujte pravidlo pre filtre politiky pre toto pripojenie. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP8629 Paket IP zrušený pre pripojenie VPN	Toto pripojenie VPN má nakonfigurované VPN NAT a vyžadovaná množina adries NAT prekročila dostupné adresy NAT.	1. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Na zväčšenie počtu adries NAT priradených pre toto pripojenie VPN použite aplikáciu iSeries Navigator. 3. Opravte všetky chyby a skúste požiadavku znova.
TCP862A Spustenie pripojenia PPP zlyhalo	Toto pripojenie VPN bolo priradené k profilu PPP. Keď bolo spustené, vykonal sa pokus o spustenie profilu PPP, ale nastalo zlyhanie.	1. V protokole úloh vyhľadajte ďalšie správy patriace tomuto pripojeniu. 2. Skontrolujte protokol úloh spojený s pripojeným PPP. 3. Opravte všetky chyby a skúste požiadavku znova.

Odstraňovanie problémov s VPN so sledovaním komunikácie OS/400

iSeries(TM) OS/400(R) poskytuje schopnosť sledovania údajov na komunikačnej linke, akou je rozhranie LAN (local area network) alebo WAN (wide area network). Priemerný užívateľ nemusí rozumieť celému obsahu sledovaných údajov. 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 vyrovnávacej pamäte)
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, pri použití väčšej veľkosti vyrovnávacej pamäte, ako je definované v SST, môžete na príkaze STRCMNTRC dostať chybovú správu. Nezabudnite, že suma veľkostí vyrovnávacej pamäte na všetkých spustených komunikačných sledovaniach nesmie prekročiť maximálnu veľkosť vyrovnávacej pamäte definovanej v SST.

DTADIR (Smer 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 sa sledovanie vráti môžete stratiť dôležité informácie o sledovaní. 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 (Popis 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 sledovaných údajov
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 vysielané údaje)
Či sa budú tlačiť všetky vysielané rámiky. Predvolená hodnota je Áno. Ak napríklad nechcete požiadavky protokolu Address Resolution Protocol (ARP), zadajte *NO. V opačnom prípade môžete byť zaplavený vysielanými správami.

Súvisiace informácie pre VPN

Viac návrhov konfigurácie a popisov VPN nájdete v týchto zdrojoch informácií:

- **OS/400(R) V5R1 Virtuálne súkromné siete: Vzdialený prístup k serveru IBM(R) e(logo)server iSeries(TM) pomocou klientov VPN (R) 2000, REDP0153**

  Táto publikácia IBM Redpaper poskytuje návod na konfiguráciu tunela VPN pomocou V5R1 VPN a integrovanej podpory L2TP a IPSec systému Windows 2000.
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  Tento redbook skúma koncepty VPN a popisuje jej implementáciu pomocou bezpečnosti IP (IPSec) a Tunelovacieho protokolu vrstvy 2 (L2TP) na OS/400.

- **Bezpečnostné návrhy pre Internet pre AS/400: Praktický prístup, SG24-5954-00**

  Táto publikácia Redbook sa týka všetkých integrovaných komponentov zabezpečenia systému OS/400, ako sú IP filtre, NAT, VPN, HTTP proxy server, SSL, DNS, mail relay, audit a protokolovanie. Pomocou praktických príkladov popisuje ich použitie.
- **Virtuálne súkromné siete: Zabezpečovanie pripojení**

  Táto webová stránka poukazuje na najhorúcejšie novinky VPN, zoznamy najnovších PTF a odkazy na ďalšie zaujímavé stránky.
- **Ostatné príručky a publikácie redbook týkajúce sa bezpečnosti**
  Tu nájdete zoznam informácií týkajúcich sa bezpečnosti, ktoré sú k dispozícii online.

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

1. Kliknite pravým tlačidlom na PDF vo vašom prehliadači (kliknite pravým tlačidlom na predchádzajúci odkaz).
2. Kliknite na **Uložiť cieľ ako...**.
3. Prejdite do adresára, v ktorom si želáte uložiť PDF.
4. Kliknite na **Uložiť**.

Ak potrebujete Adobe Acrobat Reader na zobrazovanie alebo tlač týchto súborov PDF, môžete si prevziať kópiu z webovej stránky Adobe (www.adobe.com/prodindex/acrobat/readstep.html).

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. Text tohto dokumentu vám nedáva žiadne licencie na tieto patenty. Informácie o licenciách získate u výrobcu na adrese:

```
IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY  10594-1785
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, Japan
```

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU TAK ″AKO JE″, BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY 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 49XA
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 spomínaný v týchto informáciách a všetky pre tento program dostupné licenčné materiály poskytuje spoločnosť IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement alebo ľubovoľnej ekvivalentnej zmluvy medzi nami.

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.

Všetky zobrazené ceny IBM sú aktuálne odporúčané maloobchodné ceny IBM a môžu byť zmenené bez predchádzajúceho upozornenia. Ceny jednotlivých predajcov môžu byť odlišné.

Tieto informácie slúžia len na plánovacie účely. Uvedené informácie sa môžu zmeniť ešte predtým, ako bude produkt, ktorého sa týkajú, dostupný.

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.

Ochranné známky

Nasledujúce pojmy sú ochrannými známkami spoločnosti International Business Machines Corporation v USA alebo iných krajinách:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro sú ochranné známky spoločnosti International Corporation a Lotus Development Corporation v USA alebo iných krajinách.

C-bus je ochranná známka spoločnosti Corollary, Inc. v USA alebo iných krajinách.

ActionMedia, LANDesk, MMX, Pentium a ProShare sú ochranné známky alebo zaregistrované ochranné známky spoločnosti Intel Corporation v USA alebo iných krajinách.

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

SET a logo SET sú ochranné známky, ktoré sú vlastníctvom spoločnosti SET Secure Electronic Transaction LLC.

Java a všetky s ňou súvisiace ochranné známky sú ochranné známky spoločnosti Sun Microsystems, Inc. v USA alebo iných krajinách.

UNIX je zaregistrovanou ochrannou známkou spoločnosti Open Group v USA alebo iných krajinách.

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

Podmienky sťahovania a tlače publikácií

Povolenie na používanie vybratých publikácií, ktoré si chcete stiahnuť, je podmienené vaším súhlasom s nasledujúcimi podmienkami.

Osobné použitie: Tieto publikácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto publikácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. V žiadnom prípade nemôžete tieto publikácie ani žiadnu ich časť distribuovať, prezentovať alebo z nich vytvárať odvodené práce mimo vášho podniku bez výslovného súhlasu spoločnosti IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené publikácie alebo informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

IBM si vyhradzuje právo vypovedať oprávnenia uvádzané v tomto dokumente kedykoľvek, ak usúdi, že používanie týchto publikácií poškodzuje jej záujmy alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie nie sú náležite dodržiavané.

Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu. IBM NEPOSKYTUJE ŽIADNU ZÁRUKU NA OBSAH TÝCHTO PUBLIKÁCIÍ. TIETO PUBLIKÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL.

Všetky materiály sú chránené autorským právom IBM Corporation.

Stiahnutím alebo vytlačením publikácie z týchto stránok vyjadrujete svoj súhlas s týmito podmienkami.

Vytlačené v USA