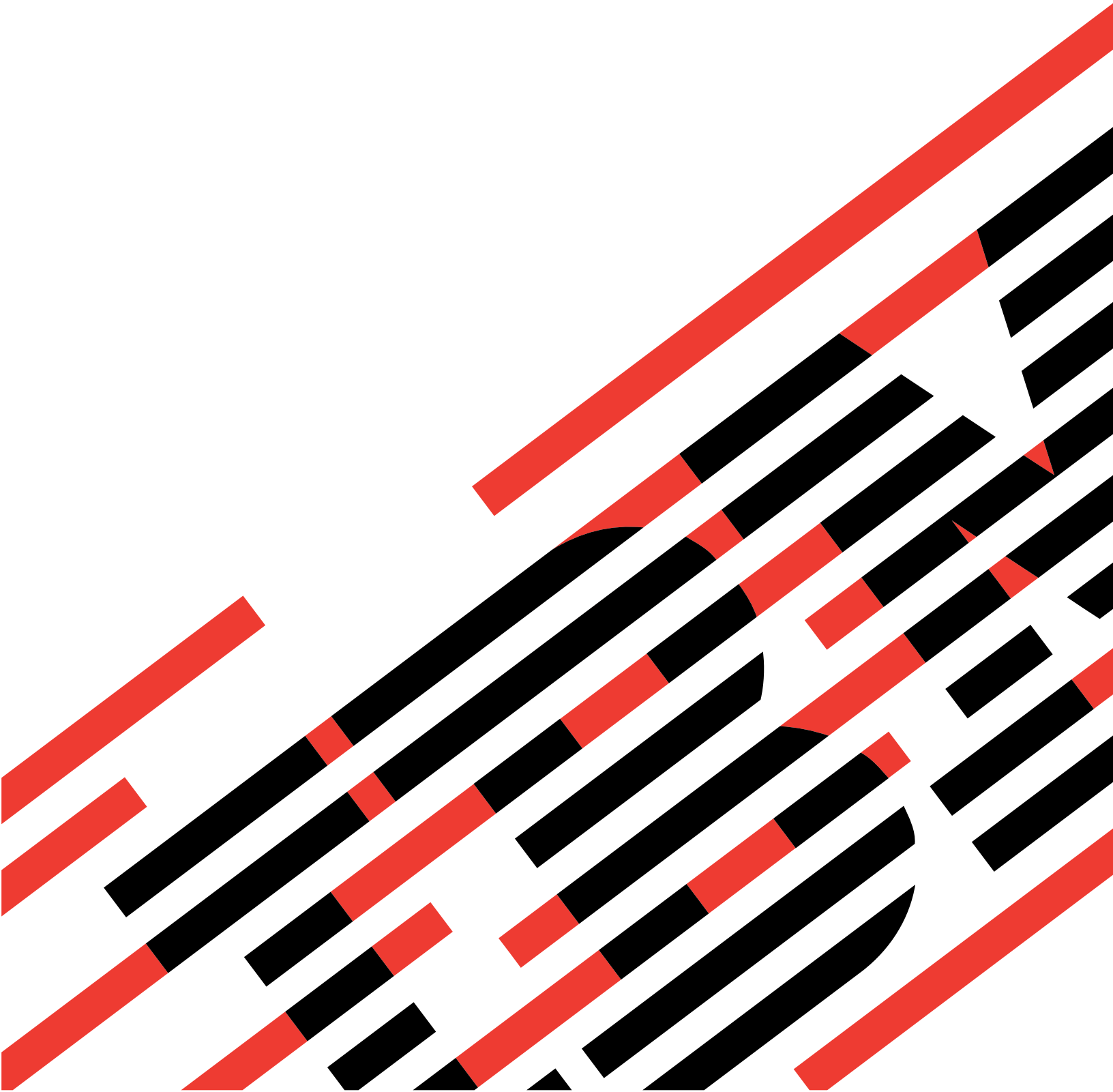
IBM

eserver

iSeries

VPN (Virtual private networking)

verze 5 vydání 3



IBM

@server

iSeries

VPN (Virtual private networking)

verze 5 vydání 3

Poznámka

Přečtěte si informace v části “Poznámky”, na stránce 67 ještě před použitím těchto informací a produktu, který podporují.

Šesté vydání (srpen 2005)

Toto vydání se vztahuje na verzi 5, vydání 3, modifikaci 2 licencovaného programu IBM i5/OS (5722-SS1) a na všechna následná vydání a modifikace, dokud nebude v nových vydáních uvedeno jinak. Tato verze není určena pro žádné modely počítačů s omezenou sadou instrukcí (RISC) ani pro modely CISC.

Obsah

VPN (Virtual Private Networking)

VPN (Virtual Private Networking) umožňuje vaší společnosti bezpečně rozšířit vnitropodnikovou síť přes existující veřejnou síť, například přes Internet. S VPN může společnost řídit provoz v síti, zatímco poskytuje důležité funkce zabezpečení, jako je například autentizace a používání soukromých údajů.

OS/400(R) VPN je volitelně instalovatelná komponenta produktu iSeries(TM) Navigator, rozhraní GUI pro systém OS/400. Umožňuje vám vytvořit zabezpečenou průběžnou cestu mezi libovolnou kombinací hostitelského systému a komunikační brány. OS/400 VPN používá k zabezpečení dat, která jsou posílána mezi dvěma koncovými systémy tohoto připojení, zásady autentizace, šifrovací algoritmy a další opatření.

VPN funguje v síťové vrstvě zásobníkového modelu úrovňové komunikace TCP/IP. Přesněji řečeno, VPN používá otevřené vývojové prostředí architektury IPSec (IP Security Architecture). IPSec dodává základní funkce zabezpečení pro Internet a poskytuje také flexibilní bloky, ze kterých můžete vytvořit robustní VPN se zabezpečením.

VPN také podporuje řešení s protokolem L2TP (Layer 2 Tunnel Protocol). Připojení L2TP, zvaná také virtuální linky, poskytují nákladově efektivní přístup vzdáleným uživatelům tím, že dovolují, aby společný síťový server spravoval IP adresy přiřazené vzdáleným uživatelům. Připojení L2TP také poskytují zabezpečený přístup k systému nebo síti, které jsou chráněné pomocí IPSec.

Je důležité, abyste pochopili, jaký vliv bude mít VPN na celou síť. Správné plánování a implementace jsou podstatou vašeho úspěchu. Prostudujte následující témata, abyste věděli, jak VPN fungují a jak byste je měli používat:

Co je nového ve verzi V5R3
Toto téma popisuje, které informace jsou v tomto vydání nové nebo významně změněné.

Tisk tohoto tématu
Dáváte-li přednost tištěné verzi, přejděte na toto téma a vytiskněte soubor PDF.

Scénáře VPN
Prostudujte tyto scénáře a seznamte se se základními typy VPN a postupy při jejich konfiguraci.

Koncepce VPN
Je důležité mít alespoň základní znalost standardních technologií VPN. Toto téma poskytuje konceptuální informace o protokolech, které VPN používá při implementaci.

Plán pro VPN
Prvním krokem úspěšného používání VPN je plánování. Toto téma poskytuje informace o migraci z předchozích vydání, požadavcích na nastavení a odkazech na poradce při plánování, který vytvoří pracovní formulář a upraví ho podle vašich specifikací.

Konfigurace VPN
Až dokončíte plánování pro VPN, můžete začít s konfigurováním. Toto téma popisuje, co všechno můžete s VPN provádět a jak na to.

Správa VPN
Toto téma popisuje mnoho různých úkolů, které můžete provádět při správě aktivních připojení VPN, například jak provádět jejich změny, jak je monitorovat nebo vymazat.

Odstraňování problémů s VPN
Máte-li problémy s připojením do VPN, prostudujte toto téma.

Související informace pro VPN
Zde najdete odkazy na jiné zdroje informací o VPN a související témata.

Co je nového ve verzi V5R3

Rozšíření funkčnosti
Rozšíření funkčnosti VPN (Virtual Private Networking) ve verzi 5, vydání 3 (V5R3) zahrnuje dva nové typy identifikátorů: Když pro VPN definujete zásady IKE a datové koncové systémy a koncové systémy připojení, můžete vybrat jeden ze dvou nových typů identifikátorů. Tyto typy identifikátorů obsahují lokální IP adresu a hostitelské jméno IPv4. Další informace najdete v online nápovědě k produktu iSeries(TM) Navigator.

- **Moje lokální IP adresa**
  Typ identifikátoru Moje lokální IP adresa můžete vybrat, když chcete definovat typ lokálního klíčového serveru pro zásadu IKE nebo lokální datový koncový systém v definici připojení. Je-li tento typ vybrán, VPN používá dostupnou IPv4 adresu. Připojení VPN, která používají tento typ identifikátoru, nesmějí používat filtr zásad. Navíc musí být lokální systém iniciátorem připojení.
- **Jméno hostitele IPv4**
  Typ identifikátoru Jméno hostitele IPv4 můžete použít, chcete-li definovat několik různých parametrů:
  – typ identifikátoru Vzdálený klíčový server v zásadě IKE
  – identifikátor Vzdálená adresa ve vlastnostech připojení
  – definici filtru zásad pro vlastnosti skupiny připojení

  Typ identifikátoru Jméno hostitele IPv4 rozhoduje o IP adrese hostitelského jména zadaného jako tento typ identifikátoru.

Upozornění zabezpečení VPN:
Kdykoli je při autentizaci použit předem nasdílený klíč, doporučuje se používat vyjednávání v hlavním režimu. Tato vyjednávání poskytují lépe zabezpečenou výměnu. Pokud musíte použít předem nasdílený klíč a vyjednávání v agresívním režimu, vyberte si záhadná slova, která bude obtížné zachytit při napadení, která snímají slovník. Chcete-li při výměně klíčů vynutit použití vyjednávání v hlavním režimu, prostudujte pokyny v části Bezpečnostní riziko s autentizací předem nasdíleného klíče. Když vytváříte nebo upravujete zásadu IKE, můžete podrobnější informace najít v nápovědě online produktu iSeries Navigator.

Rozšíření informací
Změny tématu v aplikaci Information Center pro VPN verze 5, vydání 3 (V5R3) zahrnují vizuální prezentaci vysvětlení konceptu nepovinného tunelu L2TP (Layer 2 Tunnel Protocol). Použijte následující odkaz, chcete-li prohlížet vizuální prezentaci o nepovinném tunelu L2TP chráněném pomocí IPSec. K tomu potřebujete program Flash plug-in

. Nebo můžete použít HTML verzi této prezentace.

Jak zjistíte, co je nového, nebo co se změnilo

K usnadnění přehledu o tom, kde byly provedeny technické změny, jsou použity tyto konvence:

- Obrázek

  označuje, kde nové nebo změněné informace začínají.
- Obrázek

  označuje, kde nové nebo změněné informace končí.

Další informace o tom, co je nového nebo co se změnilo, uvádí téma Sdělení pro uživatele.

Tisk tohoto tématu

Chcete-li prohlížet nebo stáhnout PDF verzi tohoto dokumentu, klepněte na odkaz VPN (Virtual Private Networking) (přibližně 509 KB).

Uložení PDF souborů

Chcete-li uložit PDF soubor na pracovní stanici, abyste ho později mohli prohlížet nebo tisknout, postupujte takto:

1. Klepněte pravým tlačítkem na PDF soubor v prohlížeči (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na příkaz **Uložit cíl jako...**, používáte-li Internet Explorer. Klepněte na příkaz **Uložit cíl jako...**, používáte-li Netscape Communicator.
3. Určete adresář, do kterého chcete PDF soubor uložit.
4. Klepněte na tlačítko **Uložit**.

Stažení programu Adobe Acrobat Reader

Chcete-li tyto soubory PDF prohlížet nebo tisknout, potřebujete program Adobe Acrobat Reader. Můžete ho stáhnout z webové stránky Adobe Web site (www.adobe.com/products/acrobat/readstep.html)

.

Scénáře VPN

Prostudujte tyto scénáře a seznamte se s technickými a konfiguračními podrobnostmi, které jsou začleněny do každého z těchto základních typů připojení:

- **Scénář VPN: Základní připojení pobočky**
  V tomto scénáři chce vaše společnost vytvořit VPN mezi podsítěmi svých vzdálených oddělení prostřednictvím páru serverů iSeries(TM), které mají roli komunikačních bran.
- **Scénář VPN: Základní připojení B2B (business to business)**
  V tomto scénáři chce vaše společnost vytvořit VPN mezi klientskou pracovní stanicí v oddělení výroby a klientskou pracovní stanicí v oddělení dodávek u vašeho obchodního partnera.
- **Scénář VPN: Ochrana nepovinného tunelu L2TP pomocí IPSec**
  Tento scénář znázorňuje připojení mezi hostitelským systémem pobočky a společnou kanceláří, která používá tunel L2TP chráněný pomocí IPSec. Pobočka má dynamicky přiřazené IP adresy, zatímco společná kancelář má statické globálně směrovatelné IP adresy.
- **Scénář VPN: Použití převodu síťových adres pro VPN**
  V tomto scénáři chce vaše společnost vyměňovat citlivá data s jedním z obchodních partnerů pomocí OS/400(R) VPN. K další ochraně soukromých údajů své síťové struktury použije společnost také převod síťových adres VPN (VPN NAT), aby skryla soukromou IP adresu serveru iSeries, který používá jako hostitelský systém aplikací, ke kterým má obchodní partner přístup.

Další scénáře VPN

Další scénáře a popisy konfigurace VPN najdete v těchto zdrojích informací:

- **Scénář QoS: Zabezpečené a předvídatelné výsledky (VPN a QoS)**
  S VPN můžete vytvořit zásady QoS (Quality of Service). Tento příklad ukazuje dvě z nich použité současně.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153**

  Tato červená kniha IBM poskytuje podrobný popis procesu konfigurace tunelu VPN pomocí VPN verze V5R1 a integrované podpory protokolů L2TP a IPSec v operačním systému Windows 2000.

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

  Tato červená kniha zkoumá koncepty VPN a popisuje implementaci VPN pomocí IPSec (IP security) a protokolu L2TP (Layer 2 Tunneling Protocol) v operačním systému OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  Tato červená kniha zkoumá všechny integrované síťové funkce zabezpečení, které jsou k dispozici v systému OS/400, například IP filtry, převod síťových adres (NAT), VPN, HTTP proxy server, SSL, DNS, přenos pošty, prověřování a protokolování. Popisuje jejich použití na praktických příkladech.

Scénář VPN: Základní připojení pobočky

Předpokládejme, že vaše firma chce minimalizovat náklady vzniklé komunikací ve vlastních pobočkách a mezi těmito pobočkami. Vaše firma používá v současné době přenosy rámců nebo pronajaté linky, ale chtěli byste zjistit další možnosti pro přenos interních důvěrných dat, které by byly méně nákladné a zajišťovaly by větší bezpečnost a globální přístupnost. Pomocí Internetu můžete snadno vytvořit síť VPN (virtual private network), která bude vyhovovat potřebám firmy.

Vaše firma i její pobočky budou potřebovat ochranu VPN po celém Internetu, ne však uvnitř jednotlivých sítí intranet. Protože sítě intranet považujete za důvěryhodné, je nejlepším řešením vytvoření VPN typu komunikační brána - komunikační brána. V tomto případě jsou obě komunikační brány připojeny přímo na zprostředkující síť. Jinými slovy, jedná se o *hraniční* nebo *okrajové* systémy, které nejsou chráněny pomocí ochranných bariér (firewall). Tento příklad slouží jako užitečný úvod k postupu, který je obsažen v nastavení základní konfigurace VPN. Když se tento scénář vztahuje k termínu *Internet*, týká se zprostředkující sítě mezi dvěma komunikačními branami VPN, kterou by mohla být vlastní soukromá síť firmy nebo veřejná síť Internet.

> **Důležitá poznámka:**
> Tento scénář ukazuje bezpečnostní komunikační brány serveru iSeries(TM) připojené přímo na Internet. Absence ochranné bariéry (firewall) má za úkol zjednodušit scénář. Neznamená to, že použití ochranné bariéry není nutné. Ve skutečnosti musíte zvážit všechna bezpečnostní rizika spojená s každým připojením k Internetu. Podrobný popis různých metod, jak snížit tato rizika, najdete v červené knizeAS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> .

Výhody

Tento scénář má následující výhody:

- Použití Internetu nebo stávajícího intranetu snižuje náklady na soukromé linky mezi vzdálenými podsítěmi.
- Použití Internetu nebo stávajícího intranetu snižuje složitost instalace a údržby soukromých linek a přiřazeného vybavení.
- Použití Internetu umožňuje připojení vzdálených systémů téměř kdekoli na světě.
- Použití VPN poskytuje uživatelům přístup ke všem serverům a zdrojům na obou koncích propojení přesně stejně, jako by byly připojeny prostřednictvím pronajaté linky nebo sítě WAN (wide area network).
- Použití standardního šifrování a metod autentizace zajišťuje zabezpečení ochrany citlivých informací, které jsou předávány z jednoho místa na druhé.
- Dynamická a pravidelná výměna kódovacích klíčů usnadňuje nastavení a minimalizuje riziko dekódování klíčů a porušení zabezpečení ochrany dat.
- Použití soukromých IP adres v každé vzdálené podsíti eliminuje nutnost přidělit každému klientovi platnou veřejnou IP adresu.

Cíle

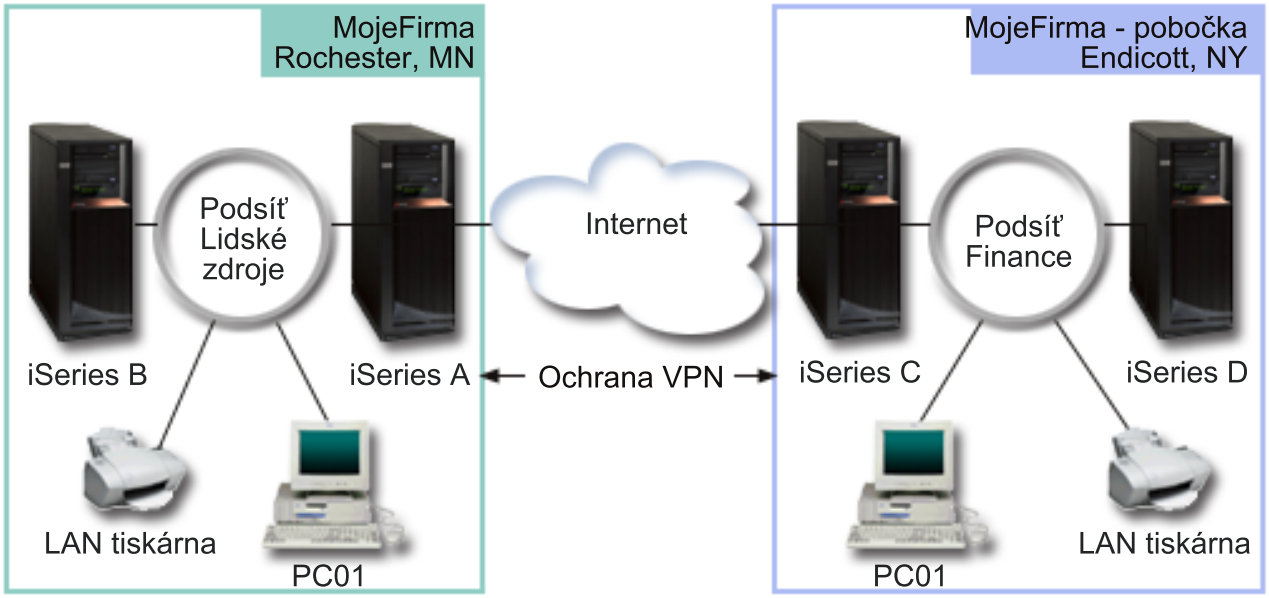
V tomto scénáři chce společnost MyCo, Inc. vytvořit VPN mezi podsítěmi svého personálního a finančního oddělení prostřednictvím páru serverů iSeries. Oba tyto servery budou mít roli komunikačních bran VPN. V termínech konfigurace VPN provádí komunikační brána správu klíčů a používá IPSec na data, která procházejí tunelem. Komunikační brány nejsou koncovými systémy připojení.

Cíle tohoto scénáře:

- VPN musí chránit veškerý provoz mezi podsítěmi personálního a finančního oddělení.
- Přenos dat nevyžaduje ochranu VPN, když dosáhne podsítě jednoho z oddělení.
- Všichni klienti a hostitelské systémy v každé síti mají úplný přístup k sítím ostatních včetně všech aplikací.
- Každý server komunikační brány může komunikovat s každým jiným serverem komunikační brány a má přístup k jeho aplikacím.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítě společnosti MyCo.



Personální oddělení

- Server iSeries-A pracuje v systému OS/400(R) verze 5, vydání 2 (V5R2) a má roli komunikační brány VPN personálního oddělení.
- Podsíť je 10.6.0.0 s maskou 255.255.0.0. Tato podsíť představuje datový koncový systém tunelu VPN na serveru společnosti MyCo Rochester.
- Server iSeries-A je připojen k Internetu s IP adresou 204.146.18.227. Toto je koncový systém připojení. Server iSeries-A tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy.
- Server iSeries-A je ke svým podsítím připojen s IP adresou 10.6.11.1.
- Server iSeries-B je provozní server v podsíti personálního oddělení, který provozuje standardní aplikace TCP/IP.

Finanční oddělení

- Server iSeries-C pracuje v systému OS/400 verze 5, vydání 2 (V5R2) a má roli komunikační brány VPN finančního oddělení.

- Podsíť je 10.196.8.0 s maskou 255.255.255.0. Tato podsíť představuje datový koncový systém tunelu VPN na serveru společnosti MyCo Endicott.
- Server iSeries-C je připojen k Internetu s IP adresou 208.222.150.250. Toto je koncový systém připojení. Server iSeries-C tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy.
- Server iSeries-C je ke své podsíti připojen s IP adresou 10.196.8.5.

Úkoly konfigurace

Chcete-li konfigurovat připojení pobočky popsané v tomto scénáři, musíte provést každý z následujících kroků:

1. Ověřte směrování protokolu TCP/IP, aby bylo zajištěno, že oba servery - komunikační brány spolu mohou komunikovat přes Internet. To také umožní zajistit, aby hostitelské systémy každé podsítě určily správně přenosovou cestu k odpovídající komunikační bráně pro přístup ke vzdálené podsíti.
   Poznámka: Určení přenosové cesty přesahuje rámec tohoto tématu. Odpovědi na případné dotazy najdete v aplikaci Information Center pod heslem Směrování TCP/IP a vyvažování zatížení.
2. Vyplňte (strana 6) pracovní formuláře a kontrolní seznamy pro plánování pro oba systémy.
3. Proveďte konfiguraci (strana 7) VPN v komunikační bráně VPN pro personální oddělení (iSeries-A).
4. Proveďte konfiguraci (strana 8) VPN v komunikační bráně VPN pro finanční oddělení (iSeries-C).
5. Ujistěte se, že servery VPN jsou spuštěny (strana 8).
6. Otestujte (strana 8) komunikaci mezi oběma vzdálenými podsítěmi.

Podrobnosti ke konfiguraci

Po dokončení prvního kroku, ve kterém jste ověřili, že směrování TCP/IP pracuje správně a že servery-brány mohou komunikovat, můžete zahájit konfiguraci VPN.

Krok 2: Vyplnění pracovních formulářů pro plánování VPN

Následující kontrolní seznamy pro plánování znázorňují typ informací, které potřebujete, než začnete s konfigurováním VPN. V nastavení VPN můžete pokračovat pouze tehdy, pokud všechny odpovědi v kontrolním seznamu jsou ANO.

Poznámka: Tyto pracovní formuláře použijte na server iSeries-A, opakujte tento postup pro server iSeries-C s příslušnými IP adresami.

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte operační systém OS/400(R) V5R2 (5722-SS1) nebo novější?	Ano
Máte nainstalovaný produkt Digital Certificate Manager (5722-SS1, volba 34)?	Ano
Máte nainstalovaný produkt Cryptographic Access Provider (5722-AC2 nebo AC3)?	Ano
Máte nainstalovaný produkt iSeries(TM) Access for Windows(R) (5722-XE1)?	Ano
Máte nainstalovaný produkt iSeries Navigator?	Ano
Máte nainstalovanou podkomponentu Network produktu iSeries Navigator?	Ano
Máte nainstalovaný produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano
Máte na serveru iSeries konfigurován protokol TCP/IP (včetně rozhraní protokolu IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény)?	Ano
Je mezi požadovanými koncovými systémy zavedena normální komunikace prostřednictvím protokolu TCP/IP?	Ano
Provedli jste nejnovější opravy PTF?	Ano
Jestliže tunel VPN prochází ochrannými bariérami (firewall) nebo směrovači, které používají filtrování IP paketů, podporují filtrovací pravidla ochranných bariér a směrovačů protokoly AH a ESP?	Ano

Kontrolní seznam nezbytných předpokladů	Odpovědi
Jsou ochranné bariéry nebo směrovač konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	Ano
Jsou ochranné bariéry konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Informace potřebné pro konfiguraci VPN	Odpovědi
Jaký typ připojení vytváříte?	komunikační brána - komunikační brána
Jak pojmenujete skupinu dynamických klíčů?	HRgw2FINgw
Jaký typ zabezpečení a provozu v systému vyžadujete pro ochranu klíčů?	Vyvážený
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Žádný topsecretstuff
Jaký je identifikátor lokálního klíčového serveru?	IP adresa: 204.146.18.227
Jaký je identifikátor lokálního datového koncového systému?	Podsíť: 10.6.0.0 Maska: 255.255.0.0
Jaký je identifikátor vzdáleného klíčového serveru?	IP adresa: 208.222.150.250
Jaký je identifikátor vzdáleného datového koncového systému?	Podsíť: 10.196.8.0 Maska: 255.255.255.0
Jaké porty a protokoly chcete povolit pro tok dat připojením?	Libovolné
Jaký typ zabezpečení a provozu v systému vyžadujete pro ochranu klíčů?	Vyvážený
Na která rozhraní budou připojení použita?	TRLINE

Krok 3: Konfigurace VPN na serveru iSeries-A

Použijte informace z pracovních formulářů a konfigurujte VPN na serveru iSeries-A takto:

1. V produktu iSeries Navigator rozbalte server iSeries-A **—>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Nové připojení**. Tím spustíte Průvodce novým připojením.
3. Informace o tom, které objekty průvodce vytváří, najdete na straně **Vítejte**.
4. Klepnutím na tlačítko **Další** přejdete na stranu **Jméno připojení**.
5. Do pole **Jméno** zadejte HRgw2FINgw.
6. (volitelné) Zadejte popis této skupiny připojení.
7. Klepnutím na tlačítko **Další** přejděte na stranu **Scénář připojení**.
8. Vyberte **Připojit vaši komunikační bránu k jiné komunikační bráně**.
9. Klepnutím na tlačítko **Další** přejděte na stranu **Zásada vzájemné výměny klíčů po Internetu**.
10. Vyberte **Vytvořit novou zásadu** a potom vyberte **Vyvážené zabezpečení a výkon**.
11. Klepnutím na tlačítko **Další** přejděte na stranu **Certifikát pro lokální koncový systém připojení**.
12. Vyberte **Ne**, což znamená, že při autentizaci připojení nebudete používat certifikáty.
13. Klepnutím na tlačítko **Další** přejděte na stranu **Lokální klíčový server**.
14. V poli **Identifikátor** vyberte **IP adresa verze 4**.
15. V poli **IP adresa** vyberte 204.146.18.227.
16. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený klíčový server**.
17. V poli **Identifikátor** vyberte **Typ identifikátoru**.
18. V poli **Identifikátor** vyberte 208.222.150.250.
19. V poli **Předem nasdílený klíč** zadejte topsecretstuff.
20. Klepnutím na tlačítko **Další** přejděte na stranu **Lokální datový koncový systém**.

21. V poli **Typ identifikátoru** vyberte **Podsíť IP verze 4**.
22. V poli **Identifikátor** vyberte 10.6.0.0.
23. V poli **Maska sítě** zadejte topsecretstuff.
24. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený datový koncový systém**.
25. V poli **Typ identifikátoru** vyberte **Podsíť IP verze 4**.
26. V poli **Identifikátor** vyberte 10.196.8.0.
27. V poli **Maska sítě** zadejte 255.255.255.0.
28. Klepnutím na tlačítko **Další** přejděte na stranu **Datové služby**.
29. Potvrďte předvolené hodnoty a potom klepnutím na tlačítko **Další** přejděte na stranu **Zásada pro práci s daty**.
30. Vyberte **Vytvořit novou zásadu** a potom vyberte **Vyvážené zabezpečení a výkon**. Vyberte **Použít k ochraně dat šifrovací algoritmus RC4**.
31. Klepnutím na tlačítko **Další** přejděte na stranu **Aplikační rozhraní**.
32. V tabulce **Linka** vyberte **TRLINE**.
33. Klepnutím na tlačítko **Další** přejděte na stranu **Souhrn**. Zkontrolujte, zda jsou průvodcem vytvořené objekty správné.
34. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci.
35. Když se zobrazí dialog **Aktivovat filtry zásad**, vyberte **Ano, aktivovat vytvořené filtry zásad** a potom vyberte **Povolit další přenosy**. Klepnutím na tlačítko **OK** dokončete konfiguraci. Na výzvu uveďte, že chcete aktivovat pravidla ve všech rozhraních.

Dokončili jste konfigurování VPN na serveru iSeries-A. Dalším krokem je konfigurace VPN v komunikační bráně VPN pro finanční oddělení (iSeries-C).

Krok 4: Konfigurace VPN na serveru iSeries-C

Postupujte stejně jako při konfiguraci serveru iSeries-A, ale s příslušnou IP adresou. Jako vodítko použijte pracovní formuláře. Když dokončíte konfigurování komunikační brány VPN pro finanční oddělení, budou připojení ve stavu *na žádost*, to znamená, že připojení bude uskutečněno, až budou odeslány IP datagramy, které toto připojení VPN musí chránit. Následující krok má za úkol spustit servery VPN, pokud ještě nejsou spuštěny.

Krok 6: Spuštění serverů VPN

Chcete-li spustit servery VPN, postupujte takto:

1. V produktu iSeries Navigator rozbalte **server —>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**.

Krok 7: Test připojení

Po dokončení konfigurování obou serverů a úspěšném spuštění serverů VPN otestujte připojitelnost, aby bylo zajištěno, že vzdálené podsítě spolu mohou komunikovat. Postupujte přitom takto:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť**.
2. Klepněte pravým tlačítkem na **Konfigurace TCP/IP** a vyberte **Obslužné programy** a potom vyberte **Testovat spojení**.
3. V dialogovém okně **Testovat spojení z** v poli **Testovat spojení** zadejte iSeries-C.
4. Klepnutím na tlačítko **Testovat spojení ihned** ověřte připojitelnost ze serveru iSeries-A na server iSeries-C.
5. Když skončíte, klepněte na tlačítko **OK**.

Scénář VPN: Základní připojení B2B (business to business)

Mnoho firem používá při zabezpečené komunikaci se svými obchodními partnery, pobočkami a dodavateli přenosy rámců nebo pronajaté linky. Tato řešení jsou často nákladná a geograficky omezená. VPN nabízí alternativu pro firmy, které chtějí vlastní nákladově efektivní komunikaci.

Předpokládejme, že jste pro výrobce dodavatelem hlavních součástek. Protože je důležité, abyste měli určité množství určitých součástek přesně v tu dobu, kdy je výrobní firma požaduje, musíte mít neustále přehled o stavu skladových zásob výrobce a o plánu výroby. Možná se touto interakcí zabýváte právě dnes a zjišťujete, že je časově náročná, nákladná a někdy dokonce nepřesná. Chcete najít jednodušší, rychlejší a efektivnější způsob komunikace s výrobní firmou. Výrobce však tyto informace nechce publikovat na firemním webu ani je nechce pravidelně distribuovat v externí sestavě kvůli důvěrné povaze vyměňovaných informací a jejich závislosti na čase. Využitím veřejné sítě Internet můžete snadno vytvořit VPN vyhovující požadavkům obou firem.

Cíle

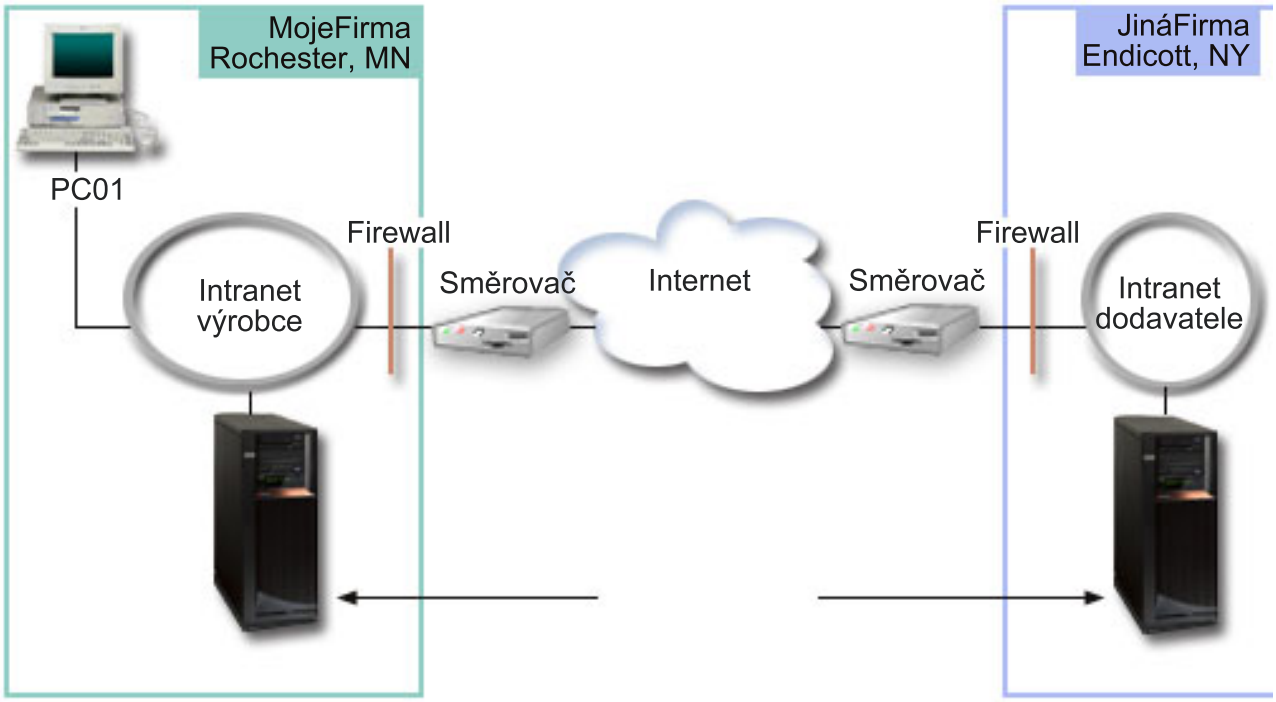
V tomto scénáři chce společnost MyCo vytvořit síť VPN mezi hostitelským systémem v sekci součástek a hostitelským systémem ve výrobním oddělení jednoho ze svých obchodních partnerů, firmy TheirCo.

Protože informace, které tyto dvě firmy sdílejí, jsou velmi důvěrné, musejí být při procházení Internetem chráněny. Data navíc nesmějí sítěmi jednotlivých firem procházet nezakódovaná, protože každá síť považuje ostatní sítě za nedůvěryhodné. Jinými slovy, obě firmy vyžadují autentizaci od místa původu do místa určení, integritu a šifrování.

Důležitá poznámka:
Tento scénář chce představit na příkladu jednoduchou konfiguraci VPN typu hostitelský systém - hostitelský systém. V obvyklém síťovém prostředí budete muset vzít v úvahu kromě jiného také konfiguraci ochranné bariéry (firewall), požadavky na IP adresy a směrování.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítí společností MyCo a TheirCo.



Dodavatelská síť společnosti MyCo

- Server iSeries-A pracuje v operačním systému OS/400(R) verze 5, vydání 2 (V5R2).
- Server iSeries-A má IP adresu 10.6.1.1. Toto je koncový systém připojení a také datový koncový systém. Server iSeries-A navazuje připojení IKE a používá IPSec na příchozí a odeslané IP datagramy a je také zdrojem i cílem pro data, která procházejí VPN.

- Server iSeries-A je v podsíti 10.6.0.0 s maskou 255.255.0.0
- Pouze server iSeries-A může iniciovat připojení k serveru iSeries-C.

Výrobní síť společnosti TheirCo

- Server iSeries-C pracuje v operačním systému OS/400 verze 5, vydání 2 (V5R2).
- Server iSeries-C má IP adresu 10.196.8.6. Toto je koncový systém připojení a také datový koncový systém. Server iSeries-A navazuje připojení IKE a používá IPSec na příchozí a odeslané IP datagramy a je také zdrojem i cílem pro data, která procházejí VPN.
- Server iSeries-C je v podsíti 10.196.8.0 s maskou 255.255.255.0

Úkoly konfigurace

Chcete-li konfigurovat připojení B2B (business to business) popsané v tomto scénáři, musíte provést každý z následujících úkolů:

1. Ověřte směrování protokolu TCP/IP, aby bylo zajištěno, že servery iSeries-A a iSeries-C spolu mohou komunikovat přes Internet. To také umožní zajistit, aby hostitelské systémy každé podsítě určily správně přenosovou cestu k odpovídající bráně pro přístup ke vzdálené podsíti. Uvědomte si, že u tohoto scénáře budete muset vzít v úvahu směrování soukromých adres, což jste dříve nemuseli.

   Poznámka: Určení přenosové cesty přesahuje rámec tohoto tématu. Odpovědi na případné dotazy najdete v aplikaci Information Center pod heslem Směrování TCP/IP a vyvažování zatížení.
2. Vyplňte (strana 10) pracovní formuláře a kontrolní seznamy pro plánování pro oba systémy.
3. Proveďte konfiguraci (strana 11) VPN na serveru iSeries-A v dodavatelské síti společnosti MyCo.
4. Proveďte konfiguraci (strana 12) VPN na serveru iSeries-C ve výrobní síti společnosti TheirCo.
5. Aktivujte (strana 12) filtrovací pravidla na obou serverech.
6. Spusťte připojení (strana 12) ze serveru iSeries-A.
7. Otestujte (strana 13) komunikaci mezi oběma vzdálenými podsítěmi.

Podrobnosti ke konfiguraci

Po dokončení prvního kroku, ve kterém jste ověřili, že směrování TCP/IP pracuje správně a že servery mohou komunikovat, můžete zahájit konfiguraci VPN.

Krok 2: Vyplnění pracovních formulářů pro plánování VPN

Následující kontrolní seznamy pro plánování znázorňují typ informací, které potřebujete, než začnete s konfigurováním VPN. V nastavení VPN můžete pokračovat pouze tehdy, pokud všechny odpovědi v kontrolním seznamu jsou ANO.

Poznámka: Tyto pracovní formuláře použijte na server iSeries-A, opakujte tento postup pro server iSeries-C s příslušnými IP adresami.

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte operační systém OS/400(R) V5R2 (5722-SS1) nebo novější?	Ano
Máte nainstalovaný produkt Digital Certificate Manager (5722-SS1, volba 34)?	Ano
Máte nainstalovaný produkt Cryptographic Access Provider (5722-AC2 nebo AC3)?	Ano
Máte nainstalovaný produkt iSeries(TM) Access for Windows(R) (5722-XE1)?	Ano
Máte nainstalovaný produkt iSeries Navigator?	Ano
Máte nainstalovanou podkomponentu Network produktu iSeries Navigator?	Ano
Máte nainstalovaný produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte na serveru iSeries konfigurován protokol TCP/IP (včetně rozhraní protokolu IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény)?	Ano
Je mezi požadovanými koncovými systémy zavedena normální komunikace prostřednictvím protokolu TCP/IP?	Ano
Provedli jste nejnovější opravy PTF?	Ano
Jestliže tunel VPN prochází ochrannými bariérami (firewall) nebo směrovači, které používají filtrování IP paketů, podporují filtrovací pravidla ochranných bariér a směrovačů protokoly AH a ESP?	Ano
Jsou ochranné bariéry nebo směrovače konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	Ano
Jsou ochranné bariéry konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Informace potřebné pro konfiguraci VPN	Odpovědi
Jaký typ připojení vytváříte?	Hostitelský systém - hostitelský systém
Jak pojmenujete skupinu dynamických klíčů?	MyCo2TheirCo
Jaký typ zabezpečení a provozu v systému vyžadujete pro ochranu klíčů?	Nejvyšší
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Ano
Jaký je identifikátor lokálního klíčového serveru?	IP adresa: 10.6.1.1
Jaký je identifikátor lokálního datového koncového systému?	IP adresa: 10.6.1.1
Jaký je identifikátor vzdáleného klíčového serveru?	IP adresa: 10.196.8.6
Jaký je identifikátor vzdáleného datového koncového systému?	IP adresa: 10.196.8.6
Jaké porty a protokoly chcete povolit pro tok dat připojením?	Libovolné
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu dat?	Nejvyšší
Na která rozhraní budou připojení použita?	TRLINE

Krok 3: Konfigurace VPN na serveru iSeries-A

Použijte informace z pracovních formulářů a konfigurujte VPN na serveru iSeries-A takto:

1. V produktu iSeries Navigator rozbalte svůj server **—>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Nové připojení**. Tím spustíte Průvodce připojením.
3. Informace o tom, které objekty průvodce vytváří, najdete na straně **Vítejte**.
4. Klepnutím na tlačítko **Další** přejdete na stranu **Jméno připojení**.
5. Do pole **Jméno** zadejte MyCo2TheirCo.
6. (volitelné) Zadejte popis této skupiny připojení.
7. Klepnutím na tlačítko **Další** přejděte na stranu **Scénář připojení**.
8. Vyberte **Připojit vašeho hostitele k jinému hostiteli**.
9. Klepnutím na tlačítko **Další** přejděte na stranu **Zásada vzájemné výměny klíčů po Internetu**.
10. Vyberte **Vytvořit novou zásadu** a potom vyberte **Nejvyšší zabezpečení, nejnižší výkon**.
11. Klepnutím na tlačítko **Další** přejděte na stranu **Certifikát pro lokální koncový systém připojení**.
12. Vyberte **Ano**, což znamená, že při autentizaci připojení budete používat certifikáty. Potom vyberte certifikát, které reprezentuje server iSeries-A.
    Poznámka: Pokud chcete při autentizaci lokálního koncového systému připojení použít certifikát, musíte nejprve vytvořit certifikát v produktu DCM (Digital Certificate Manager).

13. Klepnutím na tlačítko **Další** přejděte na stranu **Identifikátor lokálního koncového systému připojení**.
14. Jako typ identifikátoru vyberte **IP adresa verze 4** . Přidružená IP adresa musí být 10.6.1.1. Tyto informace jsou zase definované v certifikátu, které vytváříte v produktu DCM.
15. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený klíčový server**.
16. V poli **Identifikátor** vyberte **Typ identifikátoru**.
17. V poli **Identifikátor** zadejte 10.196.8.6.
18. Klepnutím na tlačítko **Další** přejděte na stranu **Datové služby**.
19. Potvrďte předvolené hodnoty a potom klepnutím na tlačítko **Další** přejděte na stranu **Zásada pro práci s daty**.
20. Vyberte **Vytvořit novou zásadu** a potom vyberte **Nejvyšší zabezpečení, nejnižší výkon**. Vyberte **Použít k ochraně dat šifrovací algoritmus RC4**.
21. Klepnutím na tlačítko **Další** přejděte na stranu **Rozhraní aplikací**.
22. Vyberte **TRLINE**.
23. Klepnutím na tlačítko **Další** přejděte na stranu **Souhrn**. Zkontrolujte, zda jsou průvodcem vytvořené objekty správné.
24. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci.
25. Když se zobrazí dialog **Aktivovat filtry zásad**, vyberte **Ne, budou aktivována pravidla paketů** a potom vyberte **OK**.

V následujícím kroku zadáte, že toto připojení může iniciovat pouze server iSeries-A. K tomu stačí přizpůsobit vlastnosti skupiny dynamických klíčů, MyCo2TheirCo, které průvodce vytvořil:

1. Klepněte na **Podle skupiny** v levém podokně rozhraní VPN, v pravém podokně se zobrazí nová skupina dynamických klíčů, MyCo2TheirCo. Klepněte na ni pravým tlačítkem a vyberte **Vlastnosti**.
2. Přejděte na stranu **Zásady** a vyberte volbu **Lokální systém iniciuje připojení**.
3. Klepnutím na tlačítko **OK** uložte provedené změny.

Dokončili jste konfigurování VPN na serveru iSeries-A. Dalším krokem je konfigurace VPN na serveru iSeries-C ve výrobní síti společnosti TheirCo.

Krok 4: Konfigurace VPN na serveru iSeries-C

Postupujte stejně jako při konfiguraci serveru iSeries-A, ale s příslušnou IP adresou. Jako vodítko použijte pracovní formuláře. Po dokončení konfigurování serveru iSeries-C musíte aktivovat filtrovací pravidla, která Průvodce připojením na každém serveru vytvořil.

Krok 5: Aktivace pravidel paketů

Průvodce automaticky vytvoří pravidla paketů, která toto připojení požaduje, aby pracovalo správně. Musíte je ale aktivovat v obou systémech ještě před připojením do VPN. Na serveru iSeries-A je můžete aktivovat takto:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketů** a vyberte **Aktivovat**. Otevře se dialog **Aktivovat pravidla paketů**.
3. Vyberte, zda chcete aktivovat pouze pravidla generovaná VPN, pouze vybraný soubor, nebo obojí. Mohli byste vybrat posledně jmenovanou možnost, máte-li mnoho různých pravidel pro povolení a odepření přístupu, která chcete kromě pravidel generovaných VPN v rozhraní používat.
4. Vyberte rozhraní, ve kterém chcete pravidla aktivovat. V tomto případě vyberte **Všechna rozhraní**.
5. Klepnutím na tlačítko **OK** v dialogu potvrdíte, že chcete pravidla ověřit a aktivovat ve vybraných rozhraních. Systém pak pravidla zkontroluje a ohlásí případné syntaktické a sémantické chyby v okně zprávy v dolní části okna editoru. Chcete-li zjistit, ke kterému souboru a číslu řádku jsou chybové zprávy přiřazeny, klepněte pravým tlačítkem na chybu a vyberte příkaz **Přejít na řádek**. Chyba bude v souboru zvýrazněna.
6. Stejným postupem aktivujte pravidla paketů na serveru iSeries-C.

Krok 6: Spuštění připojení

Chcete-li navázat připojení MyCo2TheirCo ze serveru iSeries-A:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť —>Zásady pro práci s IP**.
2. Není-li server VPN spuštěn, klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**. Tím se server VPN spustí.
3. Rozbalte **VPN (Virtual Private Networking) —>Zabezpečená připojení**.
4. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
5. Klepněte pravým tlačítkem na **MyCo2TheirCo** a vyberte **Spustit**.
6. V menu **Zobrazení** vyberte příkaz **Obnovit**. Je-li připojení úspěšně spuštěno, změní se stav z hodnoty *Nečinný* na *Aktivní*. Spuštění připojení může trvat až několik minut, proto pravidelně aktualizujte, dokud se stav nezmění na *Aktivní*.

Krok 7: Test připojení

Po dokončení konfigurování obou serverů a úspěšném připojení otestujte připojitelnost, aby bylo zajištěno, že vzdálené hostitelské systémy spolu mohou komunikovat. Postupujte přitom takto:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť**.
2. Klepněte pravým tlačítkem na **Konfigurace TCP/IP** a vyberte **Obslužné programy** a potom vyberte **Testovat spojení**.
3. V dialogovém okně **Testovat spojení z** v poli **Testovat spojení** zadejte iSeries-C.
4. Klepnutím na tlačítko **Testovat spojení ihned** ověřte připojitelnost ze serveru iSeries-A na server iSeries-C.
5. Když skončíte, klepněte na tlačítko **OK**.

Scénář VPN: Ochrana nepovinného tunelu L2TP pomocí IPSec

Předpokládejme, že vaše společnost má malou pobočku v jiném státu. V průběhu libovolného pracovního dne může pobočka vyžadovat přístup k důvěrným informacím o serveru iSeries(TM), které jsou na společném intranetu. V současné době poskytuje vaše společnost pobočce přístup ke společné síti prostřednictvím nákladné pronajaté linky. I když chce společnost i nadále poskytovat zabezpečený přístup k intranetu, musíte bezpodmínečně snížit náklady spojené s pronajatou linkou. Můžete to provést vytvořením nepovinného tunelu L2TP (Layer 2 Tunnel Protocol), který rozšíří vaši společnou síť tak, že se pobočka bude jevit jako součást podnikové podsítě. VPN chrání provoz tunelem L2TP.

S nepovinným tunelem L2TP vytvoří vzdálená pobočka tunel přímo do síťového serveru LNS (L2TP network server) společné sítě. Funkční vybavení koncentrátoru LAC (L2TP access concentrator) je umístěno na klientovi. Tunel je transparentní vzhledem k poskytovateli služeb sítě Internet (ISP) vzdáleného klienta, takže poskytovatel ISP nemusí podporovat protokol L2TP. Další informace o konceptech L2TP najdete v části Protokol L2TP (Layer 2 Tunnel Protocol).

> **Důležitá poznámka:**
> Tento scénář ukazuje bezpečnostní komunikační brány serveru iSeries připojené přímo na Internet. Absence ochranné bariéry (firewall) má za úkol zjednodušit scénář. Neznamená to, že použití ochranné bariéry není nutné. Musíte uvážit všechna bezpečnostní rizika spojená s každým připojením k Internetu. Podrobný popis různých zásad, které snižují tato rizika, najdete v této červené knize: AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> .

Cíle

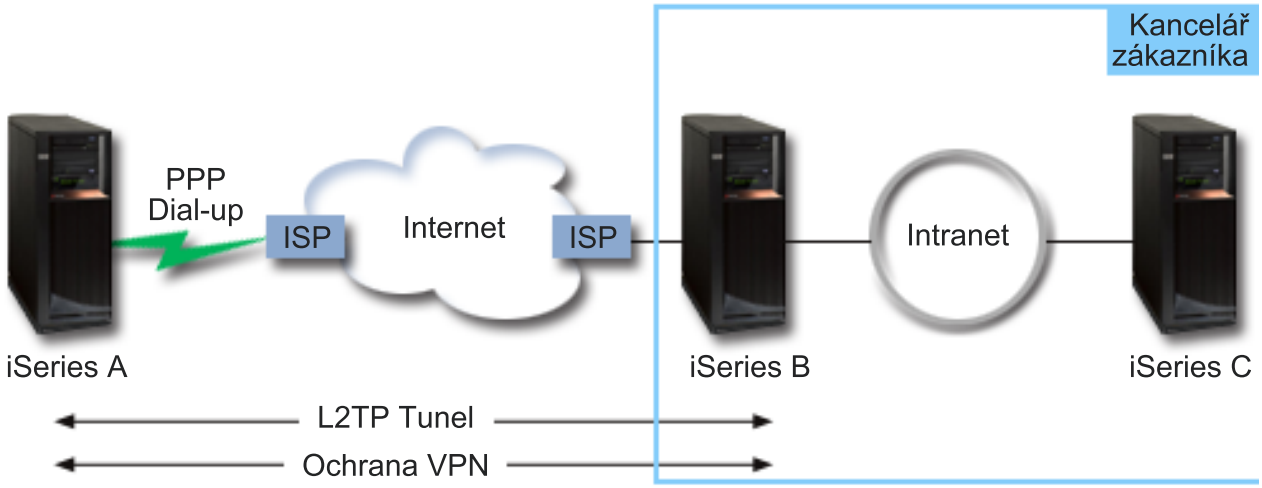
V tomto scénáři se větev serveru iSeries připojí ke společné síti přes komunikační bránu serveru iSeries s tunelem L2TP chráněným VPN.

Hlavní cíle tohoto scénáře:

- Systém pobočky vždy iniciuje připojení ke společné kanceláři.
- Systém pobočky je jediným systémem v síti pobočky, který potřebuje přístup ke společné síti. Jinými slovy, má v síti pobočky roli hostitelského systému, ne komunikační brány.
- Společný systém je hostitelský počítač ve společné síti.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítí pro tento scénář:



Server iSeries-A

- Musí mít přístup k aplikacím TCP/IP ve všech systémech ve společné síti.
- Přijímá dynamicky přiřazené IP adresy od svého poskytovatele ISP.
- Musí být konfigurován tak, aby podporoval protokol L2TP.

Server iSeries-B

- Musí mít přístup k aplikacím TCP/IP na serveru iSeries-A.
- Podsíť je 10.6.0.0 s maskou 255.255.0.0. Tato podsíť představuje datový koncový bod tunelu VPN na společném uzlu.
- Připojuje se k Internetu s IP adresou 205.13.237.6. Toto je koncový bod připojení. Server iSeries-B tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy. Server iSeries-B se ke svým podsítím připojuje s IP adresou 10.6.11.1.

V podmínkách protokolu L2TP vystupuje server *iSeries-A* jako iniciátor L2TP, zatímco server *iSeries-B* vystupuje jako terminátor L2TP.

Úkoly konfigurace

Za předpokladu, že konfigurace TCP/IP již existuje a funguje, musí být provedeny následující úkoly:

1. Konfigurace VPN (strana 15) na serveru iSeries-A.
2. Konfigurace profilu připojení PPP (strana 17) a virtuální linky pro server iSeries-A.
3. Použití (strana 18) skupiny s dynamicky přiřazeným klíčem na profil PPP.
4. Konfigurace VPN (strana 18) na serveru iSeries-B.
5. Konfigurace profilu připojení PPP (strana 18) a virtuální linky pro server iSeries-B.
6. Aktivace (strana 19) pravidel paketů na serverech iSeries-A a iSeries-B.

7. Spuštění (strana 19) připojení ze serveru iSeries-A.

Podrobnosti ke konfiguraci

Po ověření, že TCP/IP pracuje správně a že servery iSeries(TM) mohou komunikovat, můžete zahájit konfiguraci připojení popsaného v tomto scénáři.

Krok 1: Konfigurace VPN na serveru iSeries-A

Při konfiguraci VPN na serveru iSeries-A postupujte takto:

1. **Konfigurujte zásady IKE (Internet Key Exchange).**
   a. V produktu iSeries Navigator rozbalte server iSeries-A **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zásady zabezpečení IP**.
   b. Klepněte pravým tlačítkem na **Zásady IKE (Internet Key Exchange)** a vyberte **Nová zásada IKE (New Internet Key Exchange)**.
   c. Na straně **Vzdálený server** vyberte jako typ identifikátoru **IP adresa verze 4** a potom do pole **IP adresa** zadejte 205.13.237.6.
   d. Na straně **Přidružení** vyberte **Předem nasdílený klíč**, chcete-li indikovat že toto připojení používá při autentizaci této zásady připojení předem nasdílený klíč.
   e. Zadejte předem nasdílený klíč do pole **Klíč**. S předem nasdíleným klíčem zacházejte jako s heslem.
   f. Vyberte **Identifikátor klíče** pro identifikátor typu lokálního klíčového serveru a potom zadejte identifikátor do pole **Identifikátor**. Zadejte například thisisthekeyid. Uvědomte si, že lokální klíčový server má dynamicky přiřazenou IP adresu, která není předem známa. Server iSeries-B používá tento identifikátor k identifikaci serveru iSeries-A, když server iSeries-A iniciuje připojení.
   g. Klepnutím na **Přidat** na straně **Transformy** přidejte transformy, které server iSeries-A navrhne serveru serveru iSeries-B na ochranu klíče, a zadejte, zda zásada IKE používá ochranu identity při inicializaci vyjednávání fáze 1.
   h. Na straně **Transformy zásad IKE** vyberte jako metodu autentizace **Předem nasdílený klíč**, jako algoritmus přepočtu klíče **SHA** a jako šifrovací algoritmus **3DES-CBC**. Akceptujte předvolby pro skupinu Diffie-Hellman a pro Ukončit platnost klíčů IKE.
   i. Klepnutím na tlačítko **OK** se vraťte na stranu **Transformy**.
   j. Vyberte **Vyjednávání IKE v agresívním režimu (bez ochrany identity)**.

   Poznámka: Pokud v konfiguraci používáte zároveň předem nasdílené klíče a vyjednávání v agresívním režimu, vyberte si záhadná hesla, která bude obtížné zachytit při napadení, která snímají slovník. Také se doporučuje, abyste hesla pravidelně měnili.

   k. Klepnutím na tlačítko **OK** uložte konfigurace.
2. **Konfigurace zásad pro práci s daty**
   a. V rozhraní VPN klepněte pravým tlačítkem na **Zásady pro práci s daty** a vyberte **Nová zásada pro práci s daty**.
   b. Na straně **Obecné** zadejte jméno zásady pro práci s daty. Zadejte například l2tpremoteuser.
   c. Přejděte na stranu **Návrhy**. Návrh je kolekce protokolů, které iniciující a odpovídající klíčové servery používají k vytvoření dynamického připojení mezi dvěma koncovými systémy. Můžete používat jednu zásadu pro práci s daty v několika objektech připojení. Ne všechny vzdálené klíčové servery VPN však mají stejné vlastnosti zásad pro práci s daty. Proto můžete k jedné zásadě pro práci s daty přidat několik návrhů. Když vytváříte připojení VPN ke vzdálenému klíčovému serveru, musí být alespoň jeden stejný návrh v zásadě pro práci s daty iniciátora i odpovídající strany.
   d. Klepnutím na **Přidat** přidejte zásadu pro práci s daty.
   e. Chcete-li vybrat režim zapouzdření, vyberte **Přenos**.
   f. Zadejte hodnotu pro ukončení platnosti klíče.

g. Klepnutím na tlačítko **OK** se vraťte na stranu **Transformy**.

h. Klepnutím na tlačítko **OK** uložte nové zásady pro práci s daty.

3. **Konfigurace skupiny s dynamicky přiřazeným klíčem**

4.

a. V rozhraní VPN rozbalte **Zabezpečená připojení**.

b. Klepněte pravým tlačítkem na **Podle skupin** a vyberte **Nová skupina s dynamicky přiřazeným klíčem**.

c. Na straně **Obecné** zadejte jméno skupiny. Zadejte například l2tptocorp.

d. Vyberte **Chrání lokálně iniciovaný tunel L2TP**.

e. U systémové role vyberte **Oba systémy jako hostitelské**.

f. Přejděte na stranu **Zásada**. V rozbalovacím seznamu **Zásada pro práci s daty** vyberte zásadu pro práci s daty, kterou jste vytvořili v kroku 2: l2tpremoteuser.

g. Chcete-li, aby všechna připojení k serveru iSeries-B směl iniciovat pouze server iSeries-A, vyberte **Lokální systém iniciuje připojení**.

h. Přejděte na stranu **Připojení**. Vyberte **Generovat následující filtrovací pravidlo zásad pro tuto skupinu**. Klepnutím na **Editovat** definujete parametry filtru zásad.

i. Na straně **Filtr zásad - Lokální adresy** vyberte jako typ identifikátoru **Identifikátor klíče**.

j. Pro identifikátor vyberte identifikátor klíče thisisthekeyid, který jste definovali v zásadě IKE.

k. Přejděte na stanu **Filtr zásad - Vzdálené adresy**. V rozbalovacím seznamu **Typ identifikátoru** vyberte **Adresa IP verze 4**.

l. V poli **Identifikátor** zadejte 205.13.237.6.

m. Přejděte na stranu **Filtr zásad - Služby**. Do polí **Lokální port** a **Vzdálený port** zadejte hodnotu 1701. Port 1701 je pro protokol L2TP známý port.

n. V rozbalovacím seznamu **Protokol** vyberte **UDP**.

o. Klepnutím na tlačítko **OK** se vraťte na stranu **Připojení**.

p. Přejděte na stranu **Rozhraní**. Vyberte libovolnou linku nebo profil PPP, pro které bude tato skupina použita. Pro tuto skupinu jste profil PPP ještě nevytvořili. Až ho vytvoříte, musíte upravit vlastnosti této skupiny tak, aby tato skupina byla použita pro profil PPP, který vytvoříte v příštím kroku.

q. Klepnutím na tlačítko **OK** vytvořte skupinu s dynamicky přiřazeným klíčem l2tptocorp.

Potom musíte k právě vytvořené skupině přidat připojení.

5. **Konfigurace připojení s dynamicky přiřazeným klíčem**

a. V rozhraní VPN rozbalte **Podle skupin**. Tím zobrazíte seznam všech skupin s dynamicky přiřazeným klíčem, které jste konfigurovali na serveru iSeries-A.

b. Klepněte pravým tlačítkem na **l2tptocorp** a vyberte **Nové připojení s dynamicky přiřazeným klíčem**.

c. Na straně **Obecné** zadejte volitelný popis připojení.

d. U vzdáleného klíčového serveru vyberte jako typ identifikátoru **Adresa IP verze 4**.

e. V rozbalovacím seznamu **IP adresa** vyberte 205.13.237.6.

f. Zrušte označení **Spustit na žádost**.

g. Přejděte na stranu **Lokální adresy**. Pro typ identifikátoru vyberte **Identifikátor klíče** a potom v rozbalovacím seznamu **Identifikátor** vyberte thisisthekeyid.

h. Přejděte na stranu **Vzdálené adresy**. Jako typ identifikátoru vyberte **Adresa IP verze 4**.

i. V poli **Identifikátor** zadejte 205.13.237.6.

j. Přejděte na stranu **Služby**. Do polí **Lokální port** a **Vzdálený port** zadejte hodnotu 1701. Port 1701 je pro protokol L2TP známý port.

k. V rozbalovacím seznamu **Protokol** vyberte **UDP**.

l. Klepnutím na tlačítko **OK** vytvořte připojení s dynamicky přiřazeným klíčem.

Dokončili jste konfigurování VPN na serveru iSeries-A. Dalším krokem je konfigurace profilu PPP pro server iSeries-A.

Krok 2: Konfigurace profilu připojení PPP a virtuální linky na serveru iSeries-A

Tato část uvádí postup při vytváření profilu PPP pro server iSeries-A. K profilu PPP není přiřazena žádná fyzická linka. Používá místo ní virtuální linku. Důvodem je to, že provoz PPP prochází tunelem L2TP, zatímco VPN tunel L2TP chrání.

Chcete-li vytvořit profil připojení PPP pro server iSeries-A, postupujte takto:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť —>Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem na **Profily připojení původců** a vyberte **Nový profil**.
3. Na straně **Nastavení** vyberte typ protokolu **PPP**.
4. Vyberte režim **L2TP (virtuální linka)**.
5. V rozbalovacím seznamu **Provozní režim** vyberte **Iniciátor na žádost (nepovinný tunel)**.
6. Klepnutím na tlačítko **OK** přejděte na strany vlastností profilů PPP.
7. Na straně **Obecné** zadejte jméno, které určuje typ a cíl připojení. V tomto případě zadejte toCORP. Toto jméno nesmí být delší než 10 znaků.
8. (volitelné) Zadejte popis profilu.
9. Přejděte na stranu **Připojení**.
10. V poli **Jméno virtuální linky** vyberte v rozbalovacím seznamu hodnotu **tocorp**. Uvědomte si, že k této lince není přiřazeno žádné fyzické rozhraní. Virtuální linka popisuje mnoho různých charakteristik tohoto profilu PPP, například maximální velikost rámce, informace o autentizaci, jméno lokálního hostitelského systému atd. Otevře se dialog **Vlastnosti linky L2TP**.
11. Na straně **Obecné** zadejte popis virtuální linky.
12. Přejděte na stranu **Autentizace**.
13. V poli **Jméno lokálního hostitelského systému** zadejte jméno lokálního klíčového serveru iSeriesA.
14. Klepnutím na tlačítko **OK** uložte novou virtuální linku a vraťte se na stranu **Připojení**.
15. V poli **Adresa vzdáleného koncového systému tunelu** zadejte adresu vzdáleného koncového systému tunelu 205.13.237.6.
16. Vyberte **Vyžaduje ochranu IPSec** a v rozbalovacím seznamu **Jméno skupiny připojení** vyberte skupinu s dynamicky přiřazeným klíčem l2tptocorp, kterou jste vytvořili v kroku 2.
17. Přejděte na stranu **Nastavení TCP/IP**.
18. V sekci **IP adresa lokálního systému** vyberte **Přiřazená vzdáleným systémem**.
19. V sekci **IP adresa vzdáleného systému** vyberte **Použít pevnou IP adresu**. Zadejte 10.6.11.1, což je IP adresa vzdáleného systému v podsíti.
20. V sekci Směrování vyberte **Definovat další statické přenosové cesty** a klepněte na **Přenosové cesty**. Pokud profil PPP neposkytuje žádné informace o přenosové cestě, pak pro server iSeries-A je dosažitelný pouze koncový systém vzdáleného tunelu, ale žádný jiný systém v podsíti 10.6.0.0.
21. Klepnutím na tlačítko **Přidat** přidejte záznam statické přenosové cesty.
22. Zadejte podsíť 10.6.0.0 a masku podsítě 255.255.0.0, veškerý provoz 10.6.*.* tak bude přesměrován přes tunel L2TP.
23. Klepnutím na tlačítko **OK** přidejte záznam statické přenosové cesty.
24. Klepnutím na tlačítko **OK** zavřete dialog Směrování.
25. Přejděte na stranu **Autentizace** a nastavte jméno a heslo pro tento profil PPP.
26. V sekci Identifikace lokálního systému vyberte **Povolit vzdálenému systému ověřit identitu tohoto systému**.
27. V sekci **Použít autentizační protokol** vyberte **Vyžadovat šifrované heslo (CHAP-MD5)**.
28. Zadejte jméno uživatele iSeriesA a heslo.
29. Klepnutím na tlačítko **OK** uložte profil PPP.

Krok 3: Použití skupiny s dynamicky přiřazeným klíčem l2tptocorp na profil PPP toCorp

Až dokončíte konfiguraci profilu PPP, musíte se vrátit ke skupině s dynamicky přiřazeným klíčem l2tptocorp, kterou jste vytvořili a přiřadili profilu PPP. Postupujte přitom takto:

1. Přejděte do rozhraní VPN a potom rozbalte **Zabezpečená připojení—>Podle skupin**.
2. Klepněte pravým tlačítkem na skupinu s dynamicky přiřazeným klíčem l2tptocorp a vyberte **Vlastnosti**.
3. Přejděte na stranu **Rozhraní** a vyberte **Použít tuto skupinu** pro profil PPP toCorp, který jste vytvořili v kroku 2.
4. Klepnutím na tlačítko **OK** použijte l2tptocorp na profil PPP toCorp.

Krok 4: Konfigurace VPN na serveru iSeries-B

Postupujte stejně jako při konfiguraci serveru iSeries-A, ale s příslušnými IP adresami a identifikátory. Než začnete, vezměte v úvahu tyto skutečnosti:

- Označte vzdálený klíčový server identifikátorem klíče, který jste zadali pro lokální klíčový server na serveru iSeries-A, například thisisthekeyid.
- Použijte *přesně* stejný předem nasdílený klíč.
- Přesvědčte se, že vaše transformy odpovídají transformům konfigurovaným na serveru iSeries-A, jinak připojení nebudou fungovat.
- U skupiny s dynamicky přiřazeným klíčem nepoužívejte volbu **Chrání lokálně iniciovaný tunel L2TP** na straně **Obecné**.
- Připojení iniciuje vzdálený systém.
- Zadejte, že připojení se má spustit na žádost.

Krok 5: Konfigurace profilu připojení PPP a virtuální linky na serveru iSeries-B

Chcete-li vytvořit profil připojení PPP pro server iSeries-B, postupujte takto:

1. V produktu iSeries Navigator rozbalte server iSeries-B **—>Síť —>Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem na **Profily připojení odpovídající strany** a vyberte **Nový profil**.
3. Na straně **Nastavení** vyberte typ protokolu **PPP**.
4. Vyberte režim **L2TP (virtuální linka)**.
5. V rozbalovacím seznamu **Provozní režim** vyberte **Terminátor (síťový server)**.
6. Klepnutím na tlačítko **OK** zavřete strany vlastností profilu PPP.
7. Na straně **Obecné** zadejte jméno, které určuje typ a cíl připojení. V tomto případě zadejte tobranch. Toto jméno nesmí být delší než 10 znaků.
8. (volitelné) Zadejte popis profilu.
9. Přejděte na stranu **Připojení**.
10. Vyberte IP adresu koncového systému lokálního tunelu: 205.13.237.6.
11. V poli **Jméno virtuální linky** vyberte v rozbalovacím seznamu hodnotu **tobranch**. Uvědomte si, že k této lince není přiřazeno žádné fyzické rozhraní. Virtuální linka popisuje mnoho různých charakteristik tohoto profilu PPP, například maximální velikost rámce, informace o autentizaci, jméno lokálního hostitelského systému atd. Otevře se dialog **Vlastnosti linky L2TP**.
12. Na straně **Obecné** zadejte popis virtuální linky.
13. Přejděte na stranu **Autentizace**.
14. V poli **Jméno lokálního hostitelského systému** zadejte jméno lokálního klíčového serveru iSeriesB.
15. Klepnutím na tlačítko **OK** uložte novou virtuální linku a vraťte se na stranu **Připojení**.
16. Přejděte na stranu **Nastavení TCP/IP**.
17. V sekci **IP adresa lokálního systému** vyberte pevnou IP adresu lokálního systému: 10.6.11.1.
18. V sekci **IP adresa vzdáleného systému** vyberte jako způsob přiřazení volbu **Společná oblast adres**. Zadejte počáteční adresu a potom zadejte počet adres, které mohou být přiřazeny vzdálenému systému.
19. Vyberte **Povolit vzdálenému systému přístup k dalším sítím (přesměrování IP)**.

20. Přejděte na stranu **Autentizace** a nastavte jméno uživatele a heslo pro tento profil PPP.
21. V sekci Identifikace lokálního systému vyberte **Povolit vzdálenému systému ověřit identitu tohoto systému**. Otevře se dialog **Identifikace lokálního systému**.
22. V sekci **Použít autentizační protokol** vyberte **Vyžadovat šifrované heslo (CHAP-MD5)**.
23. Zadejte jméno uživatele iSeriesB a heslo.
24. Klepnutím na tlačítko **OK** uložte profil PPP.

Krok 6: Aktivace pravidel paketů

VPN automaticky vytvoří pravidla paketů, která toto připojení požaduje, aby pracovalo správně. Musíte je ale aktivovat v obou systémech ještě před připojením do VPN. Na serveru iSeries-A je můžete aktivovat takto:

1. V produktu iSeries Navigator rozbalte server **iSeries-A —>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketu** a vyberte **Aktivovat**. Otevře se dialog **Aktivovat pravidla paketů**.
3. Vyberte, zda chcete aktivovat pouze pravidla generovaná VPN, pouze vybraný soubor, nebo obojí. Mohli byste vybrat posledně jmenovanou možnost, máte-li mnoho různých pravidel pro povolení a odepření přístupu, která chcete kromě pravidel generovaných VPN v rozhraní používat.
4. Vyberte rozhraní, ve kterém chcete pravidla aktivovat. V tomto případě vyberte **Všechna rozhraní**.
5. Klepnutím na tlačítko **OK** v dialogu potvrdíte, že chcete pravidla ověřit a aktivovat ve vybraných rozhraních. Systém pak pravidla zkontroluje a ohlásí případné syntaktické a sémantické chyby v okně zprávy v dolní části okna editoru. Chcete-li zjistit, ke kterému souboru a číslu řádku jsou chybové zprávy přiřazeny, klepněte pravým tlačítkem na chybu a vyberte příkaz **Přejít na řádek**. Chyba bude v souboru zvýrazněna.
6. Opakujte tento postup, chcete-li aktivovat pravidla paketů na serveru iSeries-B.

Krok 7: Spuštění připojení

Posledním krokem je spuštění připojení. Než můžete iniciovat připojení L2TP, musíte umožnit, aby terminátor L2TP odpovídal na požadavky iniciátora. Až se přesvědčíte, že všechny požadované služby jsou již spuštěny, spusťte připojení PPP na straně terminátora. Následující postup ukazuje, jak lze spustit připojení PPP na serveru iSeries-B:

1. V produktu iSeries Navigator rozbalte server iSeries-B **—>Síť —>Služby vzdáleného přístupu**.
2. Klepnutím na **Profily připojení odpovídající strany** zobrazte v pravé podokně seznam profilů odpovídající strany.
3. Klepněte pravým tlačítkem na tobranch a vyberte **Spustit**. Po spuštění profilu připojení se okno obnoví a zobrazí stav připojení Čeká na požadavky na připojení. Server iSeries-A pak může odpovídat na požadavky na připojení L2TP ze serveru iSeries-B.

Připojení L2TP spustíte na serveru iSeries-A takto:

1. V produktu iSeries Navigator rozbalte server iSeries-A **—>Síť—>Služby vzdáleného přístupu**.
2. Klepnutím na **Profily připojení původce** zobrazte v pravé podokně seznam profilů odpovídající strany.
3. Klepněte pravým tlačítkem na **toCORP** a vyberte **Spustit**. Po spuštění profilu připojení se okno obnoví a zobrazí stav připojení Probíhá zřizování tunelu L2TP.
4. Stisknutím klávesy F5 obnovíte obrazovku. Pokud byl tunel L2TP úspěšně spuštěn, bude zobrazen stav připojení Aktivní připojení.

Scénář VPN: Použití převodu síťových adres pro VPN

Předpokládejme, že jste správce sítě malé výrobní společnosti ve Spojených státech ve státě Minneapolis. Jeden z vašich partnerů, dodavatel součástek z Chicaga, chce většinu svých obchodních aktivit s vaší společností provádět přes Internet. Je velmi důležité, aby vaše společnost měla určité množství určitých součástek přesně v tu dobu, kdy je potřebuje. Dodavatel tedy musí znát stav skladových zásob vaší společnosti a plány výroby. V současné době provádíte tuto interakci manuálně, ale zjistili jste, že tento způsob je časově náročný, nákladný a dokonce někdy i nepřesný, takže chcete mnohem více, než jen zkoumat možnosti.

Kvůli důvěrné povaze vyměňovaných informací a jejich závislosti na čase jste se rozhodli vytvořit VPN mezi sítí dodavatele a vaší podnikovou sítí. K další ochraně soukromých údajů síťové struktury společnosti jste se rozhodli skrýt soukromé IP adresy serveru iSeries(TM), který je hostitelem aplikací, k nimž má mít dodavatel přístup. Otázka zní: Jak to uděláte?

Odpověď: OS/400(R) VPN. Můžete nejen vytvořit definice připojení v komunikační bráně VPN v podnikové síti, ale provést také převod adres, abyste mohli skrýt lokální soukromé adresy. Na rozdíl od konvenčního převodu síťových adres (NAT), který změní IP adresy v přidruženích zabezpečení (VPN ale vyžaduje, aby tyto IP adresy byly funkční), provádí VPN NAT převod adres před ověřením platnosti přidružení zabezpečení tím, že adresu přiřadí k připojení, když se toto připojení spustí.

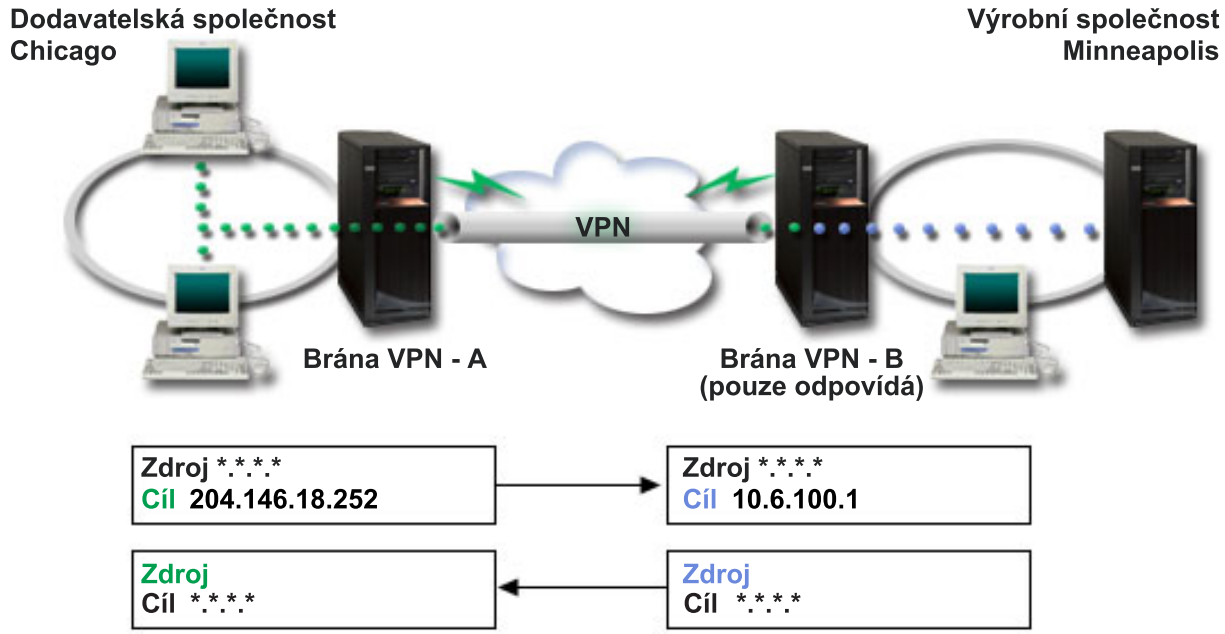
Cíle

Cíle tohoto scénáře:

- umožnit všem klientům v síti dodavatele přístup k jednomu hostitelskému serveru iSeries v síti výrobce přes připojení VPN typu komunikační brána - komunikační brána ,
- skrýt soukromé IP adresy hostitelského serveru iSeries v síti výrobce převedením na veřejné IP adresy pomocí převodu síťových adres pro VPN (VPN NAT).

Podrobnosti

Následující diagram znázorňuje síťovou charakteristiku sítě dodavatele i sítě výrobce:



- Komunikační brána VPN gateway-A je konfigurována tak, aby vždy iniciovala připojení do komunikační brány VPN gateway-B.
- Komunikační brána VPN gateway-A určuje cílový koncový systém pro připojení jako 204.146.18.252 (veřejná adresa přiřazená serveru iSeries-C).
- Soukromá IP adresa serveru iSeries-C v síti výrobce je 10.6.100.1.
- Veřejná adresa 204.146.18.252 byla definována v lokální společné oblasti služeb v komunikační bráně VPN gateway-B pro soukromou adresu serveru iSeries-C, 10.6.100.1.
- Komunikační brána VPN gateway-B převede veřejnou adresu serveru iSeries-C pro příchozí datagramy na soukromou adresu 10.6.100.1. Komunikační brána VPN gateway-B převede vrácené odchozí datagramy z adresy 10.6.100.1 zpět na veřejnou adresu serveru iSeries-C, 204.146.18.252. Pokud jde o klienty v síti dodavatele, má server iSeries-C IP adresu 204.146.18.252. Klienti nikdy nezjistí, že došlo k převodu adres.

Úkoly konfigurace

Chcete-li konfigurovat připojení popsané v tomto scénáři, musíte provést každý z následujících úkolů:

1. Konfigurace základního připojení VPN typu komunikační brána - komunikační brána mezi komunikačními bránami **VPN gateway-A** a **VPN gateway-B**.
2. Určení lokální společné oblasti služeb v komunikační bráně **VPN gateway-B** pro skrytí soukromých adres serveru **iSeries-C** do veřejného identifikátoru 204.146.18.252.
3. Konfigurace komunikační brány **VPN gateway-B** pro převod lokálních adres pomocí adres z lokální společné oblasti služeb.

Koncepce VPN

VPN používá k ochraně přenosů dat několik důležitých protokolů TCP/IP. Chcete-li lépe pochopit, jak připojení VPN pracují, seznamte se s níže uvedenými protokoly a koncepty a s tím, jak je OS/400(R) VPN používá:

- **Protokoly IPSec (IP Security)**
  IPSec poskytuje stabilní dlouhotrvající bázi pro poskytování síťového úrovňového zabezpečení.
- **Správa klíčů**
  Dynamická připojení VPN poskytují další zabezpečení komunikace tím, že používají pro správu klíčů protokol IKE (Internet Key Exchange). IKE umožňuje serverům VPN na každém konci připojení vyjednávat v zadaných intervalech nové klíče.
- **Protokol L2TP (Layer 2 Tunneling Protocol)**
  Máte-li v úmyslu používat připojení VPN při zabezpečené komunikaci mezi vaší sítí a vzdálenými klienty, musíte se seznámit také s protokolem L2TP.
- **Převod síťových adres pro VPN (VPN NAT)**
  OS/400 VPN poskytuje prostředky pro převádění síťových adres zvané VPN NAT. Liší se od tradičního převodu NAT v tom, že převádí adresy ještě před použitím protokolů IKE a IPSec. Další informace najdete v tomto tématu.
- **Zapouzdření UDP**
  Zapouzdření UDP umožňuje provozu IPSec procházet konvenčním zařízením NAT. Další informace o tom, co je zapouzdření UDP a proč byste je měli pro připojení VPN používat, najdete v tomto tématu.
- **IPComp (IP Compression)**
  Protokol IPComp snižuje velikost IP datagramů komprimací datagramů a zvyšuje tak výkon komunikace mezi dvěma partnery VPN.
- **VPN a IP filtrování**
  VPN a IP filtrování spolu úzce souvisejí. Většina připojení VPN vyžaduje pro řádné fungování filtrovací pravidla. Toto téma uvádí, jaké filtry VPN vyžaduje, a seznamuje vás s koncepty filtrování souvisejícími s VPN.

IPSec (IP Security)

IPSec poskytuje stabilní dlouhotrvající bázi pro poskytování síťového úrovňového zabezpečení. Podporuje všechny šifrovací algoritmy, které se v současné době používají, a může také pojmout nové výkonnější algoritmy, které jsou k dispozici. Protokoly IPSec věnují pozornost těmto hlavním problémům se zabezpečením:

Autentizace původních dat
Ověřuje, zda každý datagram byl vytvořen původním odesílatelem.

Integrita dat
Ověřuje, zda obsah datagramu nebyl při přenosu změněn, ať už úmyslně, nebo kvůli náhodným chybám.

Důvěrnost dat
Skryje obsah zprávy, obvykle šifrováním.

Ochrana proti zpětným dotazům
Zajišťuje, aby útočník nemohl datagram zachytit a později mu zadávat zpětné dotazy.

Automatická správa šifrovacích klíčů a přidružení zabezpečení
Zajišťuje, aby zásady VPN mohly být použity po celé rozšířené síti s co nejmenší manuální konfigurací.

VPN používá k ochraně dat, která postupují sítí VPN, dva protokoly IPSec: AH (Authentication Header) a ESP (Encapsulating Security Payload). Další částí IPSec je protokol IKE (Internet Key Exchange) neboli správa klíčů. Zatímco IPSec šifruje data, protokol IKE podporuje automatické vyjednávání přidružení zabezpečení (SA - Security Association) a automatické generování a obnovování šifrovacích klíčů.

Tento seznam uvádí nejdůležitější protokoly IPSec:

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

Společnost IETF (Internet Engineering Task Force) formálně definuje IPSec v požadavku RFC (Request for Comment) 2401, *Security Architecture for the Internet Protocol*. Tento požadavek najdete na webové stránce http://www.rfc-editor.org

.

Protokol AH (Authentication Header)

Protokol AH (Authentication Header) poskytuje datům původní autentizaci, integritu dat a ochranu proti zpětným dotazům. Neposkytuje však datům důvěrnost, což znamená, že veškerá odesílaná data jsou nezakódovaná.

Protokol AH zajišťuje integritu pomocí kontrolního součtu, který generuje kód autentizace zprávy, například MD5. Protokol AH zahrnuje ve svém algoritmu tajný nasdílený klíč, který používá při autentizaci, aby byla zajištěna autentizace původních dat. Protokol AH používá v záhlaví AH pole s pořadovými čísly, aby byla zajištěna ochrana proti zpětným dotazům. Je důležité zmínit se o tom zde, že tyto tři odlišné funkce jsou často dávány dohromady a nazývány **autentizace**. Jednoduše řečeno: Protokol AH zajišťuje, aby na cestě ke konečnému místu určení nebyla data poškozena.

I když protokol AH autentizuje IP datagram co možná nejvíce, hodnoty určitých polí v záhlaví IP nemůže příjemce předpovědět. Protokol AH tato pole, která jsou známa jako **proměnlivá** pole, nechrání. Protokol AH ale vždy chrání užitečné zatížení paketu IP.

Společnost IETF (Internet Engineering Task Force) formálně definuje protokol AH v požadavku RFC (Request for Comment) 2402, *IP Authentication Header*. Tento požadavek najdete na webové stránce http://www.rfc-editor.org

.

Způsoby použití protokolu AH

Protokol AH můžete používat dvěma způsoby: v režimu přenosu a v režimu tunelu. V režimu přenosu je záhlavím IP pro datagram nejvzdálenější záhlaví IP následované záhlavím AH a potom užitečným zatížením datagramu. Protokol AH autentizuje celý datagram kromě proměnlivých polí. Informace obsažené v datagramu jsou přenášeny nezakódované a mohou tedy být odposlouchávány. Režim přenosu vyžaduje menší režii při zpracování než režim tunelu, ale neposkytuje takové zabezpečení ochrany dat.

Režim tunelu vytvoří nové záhlaví IP a použije je jako nejvzdálenější záhlaví IP pro datagram. Záhlaví AH následuje za záhlavím IP. Původní datagram (jak záhlaví IP, tak původní užitečné zatížení) bude následovat později. Protokol AH autentizuje celý datagram, to znamená, že odpovídající systém může zjistit, zda se datagram při přenosu změnil.

Je-li komunikační brána (gateway) jedním z konců přidružení zabezpečení, použijte režim tunelu. V tomto režimu nemusí být zdrojová adresa a cílová adresa v nejvzdálenějším záhlaví IP stejná jako v původním záhlaví IP. Příklad: Dvě zabezpečené komunikační brány mohou obsluhovat tunel AH a autentizovat veškerý provoz mezi sítěmi, které propojují. Vlastně je to velmi obvyklá konfigurace.

Hlavní předností režimu tunelu je to, že dokonale chrání zapouzdřený IP datagram. Navíc umožňuje použití soukromých adres.

Proč protokol AH
V mnoha případech vyžadují data pouze autentizaci. I když protokol ESP (Encapsulating Security Payload) může provádět autentizaci, protokol AH neovlivní výkon systému tak, jako protokol ESP. Další předností použití protokolu AH je to, že autentizuje celý datagram. Protokol ESP ale neautentizuje úvodní záhlaví IP přicházející ze záhlaví ESP.

Použití protokolu ESP navíc vyžaduje silný šifrovací algoritmus. Silné šifrování je omezeno jen na některé země, zatímco použití protokolu AH není regulováno a může tedy být použit po celém světě.

Algoritmy používané protokolem AH při ochraně informací
Protokol AH používá algoritmy známé jako **kódy HMAC (hashed message authentication codes)**. Síť VPN používá buď HMAC-MD5, nebo HMAC-SHA. Oba tyto algoritmy vytvářejí výstupní data (zvaná hodnota přepočtu klíče (hash value) ze vstupních dat pevné délky a tajného klíče. Pokud se hodnoty přepočtu klíče dvou zpráv shodují, je velmi pravděpodobné, že zprávy jsou stejné. Oba algoritmy MD5 i SHA zakódují do svého výstupu délku zprávy, ale algoritmus SHA je považován za bezpečnější, protože vytvářené hodnoty přepočtu klíčů jsou větší.

Společnost IETF (Internet Engineering Task Force) formálně definuje protokol HMAC-MD5 v požadavku RFC (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Společnost IETF (Internet Engineering Task Force) formálně definuje protokol HMAC-SHA v požadavku RFC (Request for Comments) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Tyto požadavky RFC najdete na webové stránce http://www.rfc-editor.org

.

Protokol ESP (Encapsulating Security Payload)
Protokol ESP (Encapsulating Security Payload) poskytuje datům důvěrnost a také jim volitelně dává původní autentizaci, kontrolu integrity dat a ochranu proti zpětným dotazům. Rozdíl mezi protokoly ESP a AH (Authentication Header) je v tom, že protokol ESP poskytuje šifrování, zatímco oba protokoly poskytují autentizaci, kontrolu integrity dat a ochranu proti zpětným dotazům. S protokolem ESP používají oba systémy sdílený klíč pro šifrování a dekódování vyměňovaných dat.

Pokud se rozhodnete používat šifrování i autentizaci, pak systém, který odpovídá, nejprve autentizuje paket a je-li první krok úspěšný, pokračuje šifrováním. Tento typ konfigurace snižuje jak režii zpracování, tak zranitelnost v případě napadení při odepření služby.

Dva způsoby použití protokolu ESP
Protokol ESP můžete používat dvěma způsoby: v režimu přenosu a v režimu tunelu. V režimu přenosu následuje záhlaví ESP za záhlavím IP původního IP datagramu. Má-li již datagram záhlaví IPSec, pak ho záhlaví ESP předchází. Koncové návěští ESP a volitelná autentizační data následují za užitečným zatížením.

Režim přenosu neautentizuje ani nekóduje záhlaví IP, které by při přenosu datagramu mohlo vystavit informace o adresování potencionálním útočníkům. Režim přenosu vyžaduje menší režii při zpracování než režim tunelu, ale neposkytuje takové zabezpečení ochrany dat. Hostitelské systémy většinou používají protokol ESP v režimu přenosu.

Režim tunelu vytvoří nové záhlaví IP a použije je jako nejvzdálenější záhlaví IP pro datagram. Následuje záhlaví ESP a pak původní datagram (jak záhlaví IP, tak původní užitečné zatížení. Koncové návěští ESP a volitelná autentizační data následují za užitečným zatížením. Používáte-li šifrování i autentizaci, protokol ESP zcela chrání původní datagram, protože představuje data užitečného zatížení pro nový paket ESP. Protokol ESP ale nechrání nové záhlaví IP. Komunikační brány musejí protokol ESP používat v režimu tunelu.

Algoritmy používané protokolem ESP při ochraně informací
Protokol ESP používá symetrický klíč, který obě komunikující strany používají k šifrování a dekódování

vyměňovaných dat. Odesílatel a příjemce se musí dohodnout na klíči, než začne mezi nimi probíhat zabezpečená komunikace. OS/400(R) VPN používá při šifrování standardy DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 a AES (Advanced Encryption Standard).

Společnost IETF (Internet Engineering Task Force) formálně definuje standard DES v požadavku RFC (Request for Comment) 1829, *The ESP DES-CBC Transform*. Společnost IETF formálně definuje standard 3DES v požadavku RFC 1851, *The ESP Triple DES Transform*. Tyto a další požadavky RFC můžete prohlížet na webových stránkách http://www.rfc-editor.org

.

Protokol ESP používá při poskytování autentizačních funkcí algoritmy HMAC-MD5 a HMAC-SHA. Oba tyto algoritmy vytvářejí výstupní data, která nazýváme hodnota přepočtu klíče (hash value), ze vstupních dat pevné délky a tajného klíče. Pokud se hodnoty přepočtu klíče dvou zpráv shodují, je velmi pravděpodobné, že zprávy jsou stejné. Oba algoritmy MD5 i SHA zakódují do svého výstupu délku zprávy, ale algoritmus SHA je považován za bezpečnější, protože vytvářené hodnoty přepočtu klíčů jsou větší.

Společnost IETF (Internet Engineering Task Force) formálně definuje protokol HMAC-MD5 v požadavku RFC (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Společnost IETF (Internet Engineering Task Force) formálně definuje protokol HMAC-SHA v požadavku RFC (Request for Comments) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Tyto a další požadavky RFC můžete prohlížet na webových stránkách http://www.rfc-editor.org

.

Sloučení protokolů AH a ESP

VPN umožňuje sloučit protokoly AH a ESP u připojení typu hostitelský systém - hostitelský systém v režimu přenosu. Sloučení těchto protokolů chrání celý IP datagram. I když sloučení těchto dvou protokolů nabízí vyšší úroveň zabezpečení, zvýšená režie při zpracování může tuto výhodu eliminovat.

Správa klíčů

Servery VPN při každém úspěšném vyjednávání znovu generují klíče, které chrání připojení, a znesnadňují tak útočníkům zachycování informací z připojení. Používáte-li navíc dokonalé utajení do budoucna, útočníci nemohou odvodit budoucí klíče na základě informací o předchozích klíčích.

Správce klíčů VPN představuje implementaci protokolu IKE (Internet Key Exchange) od IBM(TM). Server Správce klíčů VPN podporuje automatické vyjednávání přidružení zabezpečení (SA - Security Association) a také automatické generování a obnovu šifrovacích klíčů.

Přidružení zabezpečení (SA) obsahuje informace potřebné pro použití protokolů IPSec, určuje například typy algoritmů, délku a dobu trvání klíčů, účastnické strany a režimy zapouzdření.

Šifrovací klíče, jak plyne z jejich jména, zamknou nebo ochrání vaše informace, dokud se bezpečně nedostanou do svého konečného cíle.

Poznámka: Bezpečné generování klíčů je nejdůležitějším faktorem ve vytváření bezpečných soukromých připojení. Jsou-li klíče ohroženy, pak se veškerá snaha o autentizaci a šifrování, jakkoli silná, stává zbytečnou.

Fáze správy klíčů

Správce klíčů VPN používá ve své implementaci dvě odlišné fáze.

Fáze 1
Fáze 1 vytvoří hlavní utajení, ze kterého jsou odvozeny následné šifrovací klíče, které chrání provoz uživatele. To

platí dokonce i tehdy, jestliže mezi těmito dvěma koncovými systémy neexistuje žádné zabezpečení ochrany dat. Při autentizaci vyjednávání fáze 1 i při vytváření klíčů, které chrání zprávy IKE používané během následných vyjednávání fáze 2, používá VPN buď režim podpisu RSA, nebo předem nasdílené klíče.

Předem nasdílený klíč je netriviální řetězec délky až 128 znaků. Oba koncové systémy připojení se musejí na předem nasdíleném klíči dohodnout. Výhodou použití předem nasdílených klíčů je jejich jednoduchost, nevýhodou je, že nasdílená utajovaná skutečnost musí být ještě před vyjednáváním IKE distribuována mimo pásmo zpráv, například přes telefonní linku nebo registrovanou poštou. S předem nasdíleným klíčem zacházejte jako s heslem.

Autentizace *podpisu RSA* poskytuje více zabezpečení než předem nasdílené klíče, protože tento režim používá při autentizaci digitální certifikáty. Digitální certifikáty musíte konfigurovat pomocí produktu Digital Certificate Manager (5722-SS1 volba 34). Některá řešení VPN vyžadují podpis RSA, aby systémy byly schopny spolupracovat. Například VPN v operačním systému Windows(R) 2000 používá podpis RSA jako předvolenou metodu autentizace. Podpis RSA poskytuje také větší přizpůsobitelnost než předem nasdílené klíče. Použité certifikáty musejí pocházet od vydavatelů certifikátů, kterým oba klíčové servery důvěřují.

Fáze 2
Fáze 2 vyjednává přidružení zabezpečení a klíče, které chrání aktuální výměny dat aplikací. Uvědomte si, že do této chvíle nebyla žádná aplikační data ve skutečnosti odeslána. Fáze 1 chrání zprávy fáze 2 protokolu IKE.

Po dokončení vyjednávání fáze 2 vytvoří VPN zabezpečené dynamické připojení přes síť a mezi koncovými systémy, které jste pro připojení definovali. Veškerá data, která procházejí přes VPN jsou dodávána se stupněm zabezpečení a účinnosti, který byl dohodnut klíčovými servery během procesů vyjednávání fáze 1 a fáze 2.

Obecně jsou vyjednávání fáze 1 vyjednávána denně, zatímco vyjednávání fáze 2 jsou obnovována každých 60 minut nebo dokonce každých 5 minut. Vyšší obnovovací frekvence zvyšuje zabezpečení ochrany dat, ale snižuje výkon systému. Při ochraně nejcitlivějších dat používejte krátkou dobu trvání klíčů.

Když vytvoříte dynamické VPN pomocí produktu iSeries(TM) Navigator, musíte definovat zásadu IKE, abyste umožnili vyjednávání fáze 1, a zásadu pro práci s daty, která bude řídit vyjednávání fáze 2. Můžete volitelně používat průvodce novým připojením. Průvodce automaticky vytvoří každý z konfiguračních objektů, které VPN k řádnému fungování vyžaduje, včetně zásad IKE a zásad pro práci s daty.

Doporučené publikace
Další informace o protokolu IKE (Internet Key Exchange) a správě klíčů najdete v těchto požadavcích RFC (Request for Comments) společnosti IETF (Internet Engineering Task Force):

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

Tyto požadavky RFC najdete na webové stránce http://www.rfc-editor.org

.

Protokol L2TP (Layer 2 Tunnel Protocol)

Připojení protokolu L2TP (Layer 2 Tunnel Protocol), které také nazýváme virtuální linky, poskytují nákladově efektivní přístup vzdáleným uživatelům tím, že umožňují společnému síťovému serveru spravovat IP adresy přiřazené vzdáleným uživatelům. Připojení L2TP dále poskytují zabezpečený přístup k systémům a sítím, když je používáte ve spojení s IPSec (IP Security).

Protokol L2TP podporuje dva režimy tunelu: povinný a nepovinný. Hlavní rozdíl mezi těmito dvěma tunely tvoří koncový systém. Nepovinný tunel končí u vzdáleného klienta, kdežto povinný tunel končí u poskytovatele ISP.

Pomocí **povinného tunelu** L2TP iniciuje vzdálený hostitelský systém připojení k poskytovateli služeb sítě Internet (ISP). Poskytovatel ISP pak vytvoří připojení L2TP mezi vzdáleným uživatelem a společnou sítí. I když poskytovatel ISP vytvoří připojení, rozhodnete se chránit provoz pomocí VPN. Chcete-li použít povinný tunel, musí poskytovatel ISP podporovat protokol LT2P.

Chcete-li použít **nepovinný tunel** L2TP, bude připojení vytvořeno vzdáleným uživatelem obvykle pomocí klienta pro posílání tunelem L2TP. Vzdálený uživatel pak odešle pakety L2TP svému poskytovateli ISP, který je pošle dál do společné sítě. U nepovinného tunelu nemusí poskytovatel ISP protokol L2TP podporovat. Scénář *Ochrana nepovinného tunelu L2TP pomocí IPSec* uvádí příklad, jak konfigurovat větev serveru iSeries(TM), která má být připojena ke společné síti pomocí komunikační brány serveru iSeries s tunelem L2TP chráněným pomocí VPN.

Můžete si prohlédnout vizuální prezentaci o konceptu nepovinných tunelů L2TP chráněných pomocí IPSec. Potřebujete k tomu program Flash

. Nebo můžete použít HTML verzi této prezentace.

Protokol L2TP je vlastně variací zapouzdření protokolu IP. Tunel L2TP je vytvořen zapouzdřením rámce L2TP uvnitř paketu protokolu UDP (User Datagram Protocol), který je zase zapouzdřený uvnitř IP paketu. Zdrojová a cílová adresa tohoto IP paketu určují koncové systémy připojení. Protože vnější zapouzdřující protokol je IP, můžete na sloučený IP paket použít protokoly IPSec. Tím chráníte data, která procházejí tunelem L2TP. Potom můžete rovnou použít protokol AH (Authentication Header), ESP (Encapsulated Security Payload) a IKE (Internet Key Exchange).

Téma Scénář: Konfigurace vzdáleného komutovaného připojení PPP uvádí příklad použití protokolu L2TP při připojování k IBM (R) přes univerzální připojení.

Převod síťových adres pro VPN

Převod síťových adres (NAT) vezme soukromé IP adresy a převede je na veřejné IP adresy. Můžete tak zachovat cenné veřejné adresy a zároveň umožnit hostitelským systémům v síti přístup ke službám a vzdáleným hostitelským systémům přes Internet (nebo jinou veřejnou síť).

Soukromé IP adresy mohou navíc kolidovat s podobnými příchozími IP adresami. Chcete například komunikovat s jinou sítí, ale obě sítě používají adresy 10.*.*.*, což způsobí kolizi adres a ztrátu všech paketů. Použití převodu adres (NAT) na odchozí adresy by mohlo tento problém vyřešit. Je-li však datový provoz chráněn VPN, konvenční převod síťových adres nebude fungovat, protože mění IP adresy v přidruženích zabezpečení (SA). Ale VPN vyžaduje, aby byly funkční. VPN tento problém řeší tím, že poskytuje vlastní verzi převodu síťových adres nazvanou VPN NAT. VPN NAT provádí převod adres před ověřením platnosti přidružení zabezpečení (SA) tím, že adresu přiřadí k připojení, když se toto připojení spustí. Tato adresa zůstane asociovaná s připojením, dokud toto připojení neodstraníte.

Poznámka: V současné době FTP nepodporuje VPN NAT.

Způsob použití VPN NAT
Existují dva typy VPN NAT, které byste měli vzít v úvahu, než začnete. Jsou to:

VPN NAT pro prevenci konfliktů IP adres
Tento typ VPN NAT vám umožňuje vyvarovat se možných konfliktů IP adres, když konfigurujete připojení VPN mezi sítěmi nebo systémy s podobným schématem adresování. V typickém scénáři chtějí obě společnosti vytvořit připojení VPN pomocí jednoho ze stanovených rozsahů IP adres, například 10.*.*.*. Způsob konfigurace tohoto typu VPN NAT závisí na tom, zda je server iniciátorem připojení VPN nebo odpovídající stranou. Je-li server iniciátorem připojení, převedete lokální adresy na adresy kompatibilní s adresami partnera připojení VPN.

Je-li server odpovídající stranou připojení, můžete převést vzdálené adresy vašeho partnera připojení VPN na adresy kompatibilní s vaším schématem lokálního adresování. Tento typ převodu adres konfigurujte pouze pro dynamická připojení.

VPN NAT pro skrytí lokálních adres
Tento typ VPN NAT se používá především proto, aby skryl reálné IP adresy lokálního systému převodem jeho adres na jiné adresy, které budou veřejně dostupné. Při konfigurování VPN NAT můžete určit, aby každá veřejně známá IP adresa byla převedena na adresu ze společné oblasti skrytých adres. Umožní vám to také vyvážit užitečné zatížení provozu pro jednotlivou adresu mezi více adresami. VPN NAT pro lokální adresy vyžaduje, aby byl server pro svá připojení v roli odpovídající strany.

Používejte VPN NAT pro skrytí lokálních adres, odpovíte-li ano na tyto otázky:

1. Máte jeden nebo několik serverů, ke kterým mají mít lidé přístup pomocí VPN?
2. Potřebujete být flexibilní vzhledem ke skutečným IP adresám systému?
3. Máte jednu nebo několik globálně směrovatelných IP adres?

Scénář *Použití převodu síťových adres pro VPN* poskytuje příklad, jak konfigurovat VPN NAT tak, aby lokální adresy na serveru iSeries(TM) byly skryty.

Podrobné instrukce o nastavení VPN NAT na serveru iSeries najdete v nápovědě online, která je k dispozici v rozhraní VPN v produktu iSeries Navigator.

IPSec kompatibilní s převodem síťových adres (NAT)

Problém: Konvenční převod síťových adres (NAT) přeruší VPN

Převod síťových adres (NAT) umožňuje skrýt neregistrované soukromé IP adresy za sadu registrovaných IP adres. To pomáhá chránit interní síť před vnějšími sítěmi. Převod síťových adres (NAT) také pomáhá zmírnit problém s vyčerpáním IP adres, protože mnoho soukromých adres může být reprezentováno malou sadou registrovaných adres.

Konvenční převod síťových adres (NAT) ale nefunguje na paketech IPSec, protože při průchodu paketu zařízením NAT se zdrojová adresa v paketu mění a tím ruší platnost paketu. Když k tomu dojde, přijímací koncový systém připojení VPN paket vyřadí a vyjednávání o připojeních do VPN selžou.

Řešení: Zapouzdření UDP
Stručně řečeno, zapouzdření UDP zabalí IPSec paket do nového, ale duplicitního záhlaví IP/UDP. Adresa v novém záhlaví IP bude při průchodu zařízením NAT převedena. Když potom paket dosáhne svého cíle, přijímací koncový systém odstraní dodatečné záhlaví a ponechá původní paket IPSec, který pak projde všemi dalšími ověřeními platnosti.

Zapouzdření UDP můžete použít na VPN používající protokol ESP architektury IPSec buď v režimu tunelu, nebo v režimu přenosu. Ve verzi v5r2 může server iSeries(TM) vystupovat pouze jako klient pro zapouzdření UDP. To znamená, že může pouze *iniciovat* provoz se zapouzdřením UDP.

Níže uvedený obrázek znázorňuje formát paketu ESP se zapouzdřením UDP v režimu tunelu:

Původní datagram IPv4:

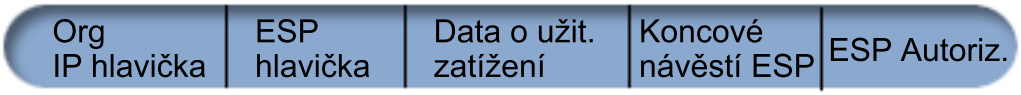
Po uplatnění IPSec ESP v režimu tunelu:

Po uplatnění zapouzdření UDP:

Níže uvedený obrázek znázorňuje formát paketu ESP se zapouzdřením UDP v režimu přenosu:

Původní datagram IPv4:

Po uplatnění IPSec ESP v režimu přenosu:



Po uplatnění zapouzdření UDP:

Server iSeries odešle po zapouzdření paket svému partnerovi VPN přes UDP port 4500. Partneři VPN provádějí obvykle vyjednávání přes UDP port 500. Když ale během vyjednávání klíčů zjistí IKE převod síťových adres (NAT), jsou následné pakety IKE odesílány přes zdrojový port 4500, cílový port 4500. To také znamená, že port 4500 nesmí být vyhrazený v žádném použitelném filtrovacím pravidle. Přijímací koncový systém připojení může stanovit, zda se jedná o paket IKE nebo o paket se zapouzdřením UDP, protože první 4 bajty užitečného zatížení UDP jsou v paketu IKE nastaveny na nulu. Pro řádné fungování musí oba koncové systémy připojení podporovat zapouzdření UDP.

IPComp (IP Compression)

Protokol IPComp (IP Payload Compression) snižuje velikost IP datagramů jejich komprimací a zvyšuje tak výkon komunikace mezi dvěma partnery. Cílem je zvýšit celkový výkon komunikace, když je vedena přes pomalé nebo zahlcené linky. Protokol IPComp neposkytuje žádné zabezpečení a když komunikace probíhá přes připojení VPN, musí být používán buď spolu s transformem AH, nebo s transformem ESP.

Společnost IETF (Internet Engineering Task Force) definuje protokol IPComp formálně v požadavku RFC (Request for Comments (RFC) 2393, *IP Payload compression Protocol (IPComp)*. Tento požadavek RFC najdete na webové stránce http://www.rfc-editor.org

.

VPN a IP filtrování

Většina připojení VPN vyžaduje pro řádné fungování filtrovací pravidla. Požadovaná filtrovací pravidla závisejí na typu připojení VPN, které konfigurujete, a také na typu provozu, který chcete řídit. Každé připojení bude obecně mít filtr zásad. Filtr zásad určuje, které adresy, protokoly a porty mohou používat VPN. Připojení, která podporují protokol IKE, mají obvykle pravidla, která jsou explicitně napsána tak, že umožňují IKE pracovat přes připojení.

Od verze V5R1 operačního systému může VPN generovat tato pravidla automaticky. Kdykoli je to možné, dovolte, ať VPN generuje filtry zásad za vás. Pomůže to eliminovat nejen chyby, ale také nutnost konfigurovat pravidla jako samostatný krok pomocí editoru pravidel paketů v produktu iSeries(TM) Navigator.

Existují ovšem výjimky. Informace o dalších, méně obvyklých konceptech a technikách VPN a filtrování, které lze použít v určité situaci, najdete v těchto tématech:

- **Migrace filtrů zásad do aktuálního vydán**
  Konfigurace pravidel paketů VPN tvořila v operačním systému verze V4R4 a V4R5 samostatný krok. Pravidla paketů nebyla generována automaticky jako součást konfigurací VPN. Toto téma podrobně popisuje zvláštní pokyny pro migraci filtrů zásad verzí V4R4 a V4R5 do aktuální verze.
- **Připojení VPN bez filtrů zásad**
  Pokud koncové systémy připojení VPN jsou samostatné specifické IP adresy a chcete spustit VPN, aniž byste v systému museli psát či aktivovat filtrovací pravidla, můžete konfigurovat dynamický filtr zásad. Toto téma vysvětluje, proč byste to měli vzít v úvahu, a naznačuje, jak to udělat.
- **Implicitní IKE**
  Má-li dojít k vyjednávání IKE pro VPN, potřebujete pro tento typ IP provozu povolit datagramy UDP přes port 500. Pokud však v systému nejsou žádná filtrovací pravidla napsaná explicitně pro povolení provozu IKE, pak systém implicitně provoz IKE povolí. V tomto tématu najdete další informace o tom, jak to funguje na serveru iSeries.

Migrace filtrů zásad na aktuální vydání

Ve verzích V4R4 a V4R5 operačního systému jste pravidla paketů VPN museli konfigurovat jako samostatný krok v rozhraní Pravidla paketů v produktu iSeries(TM) Navigator. Tato pravidla nebyla generována automaticky jako součást konfigurací VPN. Od verze V5R1 operačního systému může grafické uživatelské rozhraní GUI ve VPN vytvořit tato pravidla paketů automaticky.

V případě, že jste vytvořili filtrovací pravidla zásad (pravidla, kde akce=IPSEC) ve verzi V4R4 nebo V4R5 a chcete stejná pravidla používat v aktuální verzi, nebo v případě, že VPN *vygeneruje* filtrovací pravidla zásad, ale musíte doplnit další pravidla, která umožní ostatní IP provoz připojením, například telnet, musíte vzít v úvahu několik závažných skutečností. Budete-li se řídit následujícími doporučeními, můžete předejít možným konfiguračním chybám.

Objasnění: Odkazuje-li toto téma na soubor pravidel *zákazníka*, týká se každého souboru pravidel, který jste vytvořili pomocí editoru pravidel paketů v produktu iSeries Navigator, na rozdíl od souboru pravidel *VPNPOLICYFILTERS.I3P*, který VPN automaticky generuje jako součást konfigurace VPN.

- Máte-li připojení VPN, která jste vytvořili ve verzi V4R4 nebo V4R5, a neplánujete-li konfiguraci dalších připojení VPN v současném vydání, můžete aktivovat filtrovací pravidla a připojení jako obvykle.
- Máte-li připojení VPN, která jste vytvořili ve verzi V4R4 nebo V4R5, a plánujete-li konfiguraci dalších připojení VPN v současném vydání, použijte průvodce **Migrace filtrů zásad**. Průvodce odstraní filtry zásad ze souborů pravidel paketů, které jste vytvořili, a vloží ekvivalentní filtry zásad do souboru VPNPOLICYFILTERS.I3P, který VPN vygeneruje. Chcete-li průvodce spustit, postupujte takto:
  1. V produktu iSeries Navigator rozbalte svůj server **—>Síť —>Zásady zabezpečení IP**.
  2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Migrace filtrů zásad**.
  3. Po dokončení práce s průvodcem klepněte na tlačítko **Dokončit**.
  4. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
- Pokud filtrovací pravidla zásad generuje VPN, ale potřebujete doplnit některá filtrovací pravidla jiná než z VPN, musíte je konfigurovat pomocí editoru pravidel paketů v produktu iSeries Navigator. Pokud má libovolné filtrovací pravidlo jiné než z VPN předcházet filtry VPN, musí jméno jeho sady začínat písmeny PREIPSEC, například PREIPSECMYRULES. Systém pak snadno určí pořadí, ve kterém bude filtrovací pravidla zpracovávat. Jména sad ostatních pravidel jiných než z VPN musí mít jinou předponu než PREIPSEC, například MORERULES.
- Filtrovací pravidla zásad vždy vytvářejte pomocí VPN. Jiná filtrovací pravidla než z VPN však musejí zůstat v souboru pravidel zákazníka. Pamatujte si, že pokud má libovolné z těchto filtrovacích pravidel jiných než z VPN předcházet filtry zásad v souboru VPNPOLICYFILTERS.I3P, musíte před jméno sady doplnit předponu PREIPSEC. Tím zajistíte, aby pravidla zákazníka a pravidla VPN spolupracovala tak, jak jste měli v úmyslu.

Příklad: filtrovací pravidla zásad (sady VPN) byla vygenerována ve VPN, ale přidali jste další pravidla (vaše sady), která umožňují IP provoz připojením. Po zavedení do systému budou tato pravidla uspořádána takto:

1. Vaše sady, jejichž jména začínají písmeny PREIPSEC.
2. Sady VPN, jejichž jména začínají písmeny PREIPSEC.
3. Sady VPN s ACTION=IPSEC (filtry zásad).
4. Vaše sady s ACTION=IPSEC (filtry zásad).
5. Vaše sady s ničím jiným.
6. Sady VPN s ničím jiným.

Chcete-li si prohlédnout pořadí sloučeného výstupního souboru, zkontrolujte soubor EXPANDED.OUT. Soubor EXPANDED.OUT je zapsán do adresáře, ve kterém je umístěn soubor pravidel zákazníka.

- Pomocí produktu iSeries Navigator můžete aktivovat:
  - pouze soubor pravidel generovaných VPN, VPNPOLICYFILTERS.I3P,
  - pouze soubor pravidel zákazníka,
  - jak soubor pravidel generovaných VPN, tak soubor pravidel zákazníka.
- Aktivujte filtrovací pravidla ve všech rozhraních, ne po jednotlivých rozhraních. Zajistíte tak, že filtry budou aktivovány a také nastaveny ve správném pořadí filtrů zásad.
- Filtrovací pravidla před pokusem o aktivaci vždy prověřte. Pokud toto prověření skončí bez chyb, zkontrolujte soubor EXPANDED.OUT a přesvědčte se, že i pořadí pravidel je správné. Po dokončení tohoto kroku můžete pravidla aktivovat.

Připojení VPN bez filtrů zásad

Filtrovací pravidlo zásad určuje, které adresy, protokoly a porty mohou používat VPN a nasměruje příslušný provoz tímto připojením. V některých případech potřebujete konfigurovat připojení, které filtrovací pravidlo zásad nevyžaduje. Můžete mít například v rozhraní, které bude připojení VPN používat, zavedena jiná pravidla paketů než VPN. Rozhodnete se, že raději než deaktivovat aktivní pravidla v tomto rozhraní chcete konfigurovat VPN tak, aby všechny filtry pro připojení řídil systém dynamicky. Filtry zásad pro tento typ připojení se nazývají **dynamické filtry zásad**. Dříve než pro připojení VPN použijete dynamický filtr zásad, musí být pravdivá všechna následující tvrzení:

- Připojení může iniciovat pouze lokální server.
- Datové koncové systémy připojení musí být samostatné systémy. To znamená, že to nemohou být podsítě ani rozmezí adres.
- Pro připojení nesmí být zavedeno žádné filtrovací pravidlo zásad.

Pokud vaše připojení splňuje tato kritéria, můžete ho konfigurovat tak, že nevyžaduje filtr zásad. Při spuštění připojení budou mezi datovými koncovými systémy procházet data bez ohledu na to, jaká další pravidla paketů jsou v systému zavedena.

Podrobné instrukce o tom, jak konfigurovat připojení, aby nevyžadovalo filtr zásad, najdete v nápovědě online pro VPN.

Implicitní IKE

Chcete-li vytvořit připojení, většina VPN nejprve vyžaduje vyjednávání IKE a až potom může nastat zpracování IPSec. IKE používá známý port 500, tedy pro řádné fungování IKE potřebujete pro tento typ IP provozu povolit datagramy UDP přes port 500. Nejsou-li v systému žádná filtrovací pravidla napsaná speciálně pro povolení provozu IKE, je provoz IKE implicitně povolen. Avšak pravidla napsaná speciálně pro provoz UDP portu 500 jsou zpracovávána na základě toho, co je definováno v aktivních filtrovacích pravidlech.

Plán pro VPN

Plánování je podstatnou částí celého řešení VPN. Chcete-li zajistit, aby připojení řádně fungovalo, musíte provést mnoho složitých rozhodnutí. Shromážděte informace z níže uvedených zdrojů, abyste s VPN dosáhli úspěchu:

- **Požadavky na nastavení VPN**
  Než začnete, přesvědčte se, že pro vytvoření VPN jsou splněny minimální požadavky.

- **Určení typu VPN**
  Stanovení způsobu použití VPN je jedním z prvních kroků úspěšného plánování. Toto téma popisuje mnoho různých typů připojení, které můžete konfigurovat.
- **Použití poradce při plánování VPN**
  Poradce při plánování vám klade otázky o vaší síti a na základě vašich odpovědí podává návrhy na vytvoření VPN. **Poznámka:** Poradce při plánování používejte pouze pro připojení, která podporují protokol IKE (Internet Key Exchange). U manuálních připojení používejte pracovní formulář.
- **Vyplnění pracovních formulářů pro plánování VPN**
  Pracovní formuláře můžete vytisknout a vyplnit. Shromáždíte tak podrobné údaje o plánech na využití VPN.

Až dokončíte plánování pro VPN, můžete začít s konfigurováním.

Požadavky na nastavení VPN

Mají-li server iSeries (TM) a PC klient řádně pracovat, musejí splňovat následující požadavky:

Požadavky na server iSeries verze V5R2

- OS/400(R) verze 5, vydání 2 (5722-SS1) nebo novější.
- Digital Certificate Manager (5722-SS1 volba 34).
- Cryptographic Access Provider (5722-AC2 nebo AC3).
- iSeries Access for Windows(R)(5722-XE1) a iSeries Navigator.
  - Síťová komponenta produktu iSeries Navigator.
- Systémová hodnota QRETSVRSEC *SEC (retain server security) musí být nastavena na hodnotu 1.
- Musí být konfigurován protokol TCP/IP včetně rozhraní IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény.

Požadavky na klienta

- Pracovní stanice s 32bitovým operačním systémem Windows(R) řádně připojená k serveru iSeries a konfigurovaná pro protokol TCP/IP.
- Základní jednotka 233 MHz.
- 32 MB RAM pro klienty s operačními systémy Windows 95/98.
- 64 MB RAM pro klienty s operačními systémy Windows NT(R) a 2000.
- Produkty iSeries Access for Windows a iSeries Navigator instalované na klientském PC.
- Software podporující protokol IPSec (IP Security).
- Software podporující protokol L2TP, pokud budou vzdálení uživatelé protokol L2TP používat při vytváření připojení s vaším systémem.

Určení typu VPN

Stanovení způsobu použití VPN je jedním z prvních kroků úspěšného plánování. Potřebujete k tomu porozumět roli, kterou v připojení hraje jak lokální klíčový server, tak vzdálený klíčový server. Jsou například koncové systémy *připojení* a *datové* koncové systémy odlišné? Jsou stejné nebo kombinací obou? Koncové systémy připojení autentizují a šifrují (nebo dešifrují) provoz dat pro připojení a optimálně provádějí správu klíčů pomocí protokolu IKE. Datové koncové systémy však definují připojení mezi dvěma systémy pro IP provoz, který postupuje po VPN; například veškerý provoz TCP/IP mezi 123.4.5.6 a 123.7.8.9. Jsou-li koncové systémy připojení a datové koncové systémy odlišné, je server VPN obvykle komunikační bránou (gateway). Jsou-li stejné, je server VPN hostitelem.

Níže uvádíme různé typy implementací VPN, které vyhovují většině podnikatelských potřeb:

Komunikační brána - komunikační brána
Koncové systémy připojení obou systémů jsou odlišné od datových koncových systémů. Protokol IPSec (IP Security) chrání provoz mezi komunikačními bránami. Protokol IPSec ale nechrání provoz dat na žádné straně komunikačních brán ve vnitřních sítích. Je to běžné nastavení pro připojení mezi větvemi, protože provoz, který je směrován do vnitřních sítí za komunikační brány větvení je často považován za důvěryhodný.

Komunikační brána - hostitelský systém
Protokol IPSec chrání provoz dat mezi komunikační bránou a hostitelským systémem ve vzdálené síti. VPN nechrání provoz dat v lokální síti, protože ho považujete za důvěryhodný.

Hostitelský systém - komunikační brána
Protokol VPN chrání provoz dat mezi hostitelským systémem v lokální síti a vzdálenou komunikační bránou. VPN nechrání provoz dat ve vzdálené síti.

Hostitelský systém - hostitelský systém
Koncové systémy připojení jsou stejné jako datové koncové systémy v lokálním i vzdáleném systému. VPN chrání provoz dat mezi hostitelským systémem v lokální síti a hostitelským systémem ve vzdálené síti. Tento typ VPN poskytuje ochranu IPSec od místa původu do místa určení.

Vyplnění pracovních formulářů pro plánování VPN

Pracovní formuláře VPN vám pomohou shromáždit podrobné údaje o plánech na využití VPN. Tyto informace potřebujete, chcete-li adekvátně plánovat strategii VPN. Můžete je také použít při konfigurování VPN. Vyberte pracovní formulář pro typ připojení, který chcete vytvořit.

- **Pracovní formulář pro dynamická připojení**
  Vyplňte tento pracovní formulář ještě před konfigurováním dynamického připojení.
- **Pracovní formulář pro manuální připojení**
  Vyplňte tento pracovní formulář ještě před konfigurováním manuálního připojení.
- **Poradce při plánování VPN**
  Můžete také použít poradce, který vás interaktivně provede plánováním a konfigurací. Poradce při plánování vám klade otázky o vaší síti a na základě vašich odpovědí podává návrhy na vytvoření VPN.

  Poznámka: Poradce při plánování VPN používejte pouze u dynamických připojení. U manuálních připojení používejte pracovní formulář.

Budete-li vytvářet několik připojení s podobnými vlastnostmi, můžete nastavit předvolené hodnoty VPN. Konfigurované předvolené hodnoty naplní listy vlastností VPN. To znamená, že nebudete muset konfigurovat stejné vlastnosti několikrát. Chcete-li nastavit předvolené hodnoty VPN, vyberte z hlavního menu příkaz **Editovat** a potom vyberte **Předvolby**.

Pracovní formulář pro plánování dynamických připojení

Vyplňte tento pracovní formulář ještě před vytvořením dynamických připojení VPN. Předpokládá se přitom, že používáte průvodce novým připojením. Tento průvodce vám umožňuje nastavit VPN na základě požadavků na zabezpečení. V některých případech budete možná chtít vlastnosti konfigurované průvodcem upřesnit. Můžete se například rozhodnout, že budete vyžadovat žurnálování nebo že budete chtít, aby byl server VPN spuštěn při každém spuštění TCP/IP. V takovém případě klepněte pravým tlačítkem na skupinu nebo připojení s dynamicky přiřazeným klíčem a vyberte **Vlastnosti**.

Odpovězte na každou otázku, než budete pokračovat s nastavením VPN.

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte operační systém OS/400(R) V5R2 (5722-SS1) nebo novější?	
Máte nainstalovaný produkt Digital Certificate Manager (5722-SS1, volba 34)?	
Máte nainstalovaný produkt Cryptographic Access Provider (5722-AC2 nebo AC3)?	
Máte nainstalovaný produkt iSeries(TM) Access (5722-XE1)?	
Máte nainstalovaný produkt iSeries Navigator?	

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte nainstalovanou podkomponentu Network produktu iSeries Navigator?	
Máte nainstalovaný produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	
Máte na serveru iSeries konfigurován protokol TCP/IP (včetně rozhraní protokolu IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény)?	
Je mezi požadovanými koncovými body zavedena normální komunikace prostřednictvím protokolu TCP/IP?	
Provedli jste nejnovější opravy PTF?	
Jestliže tunel VPN prochází ochrannými bariérami (firewall) nebo směrovači, které používají filtrování IP paketů, podporují filtrovací pravidla ochranných bariér a směrovačů protokoly AH a ESP?	
Jsou ochranné bariéry nebo směrovač konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	
Jsou ochranné bariéry konfigurovány tak, že umožňují směrování pomocí IP?	

Informace potřebné pro konfiguraci dynamického připojení VPN	Odpovědi
Jaký typ připojení vytváříte? • Komunikační brána - komunikační brána • Hostitelský systém - komunikační brána • Komunikační brána - hostitelský systém • Hostitelský systém - hostitelský systém	
Jak pojmenujete skupinu dynamických klíčů?	
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu klíčů? • Nejvyšší zabezpečení, nejnižší výkon • Vyvážené zabezpečení a výkon • Nejnižší zabezpečení, nejvyšší výkon	
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	
Jaký je identifikátor lokálního klíčového serveru?	
Jaký je identifikátor lokálního datového koncového systému?	
Jaký je identifikátor vzdáleného klíčového serveru?	
Jaký je identifikátor vzdáleného datového koncového systému?	
Jaký typ zabezpečení a provozu v systému vyžadujete pro ochranu klíčů? • Nejvyšší zabezpečení a nejnižší výkon • Vyvážené zabezpečení a výkon • Nejnižší zabezpečení a nejvyšší výkon	

Pracovní formulář pro manuální připojení

Vyplňte tento pracovní formulář. Pomůže vám vytvořit připojení VPN, která pro správu klíčů nepoužívají IKE.

Odpovězte na každou otázku, než budete pokračovat s nastavením VPN:

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte operační systém OS/400(R) V5R2 (5722-SS1) nebo novější?	
Máte nainstalovaný produkt Digital Certificate Manager (5722-SS1, volba 34)?	

Kontrolní seznam nezbytných předpokladů	Odpovědi
Máte nainstalovaný produkt Cryptographic Access Provider (5722-AC2 nebo AC3)?	
Máte nainstalovaný produkt iSeries(TM) Access (5722-XE1)?	
Máte nainstalovaný produkt iSeries Navigator?	
Máte nainstalovanou podkomponentu Network produktu iSeries Navigator?	
Máte nainstalovaný produkt TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	
Máte na serveru iSeries konfigurován protokol TCP/IP (včetně rozhraní protokolu IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény)?	
Je mezi požadovanými koncovými body zavedena normální komunikace prostřednictvím protokolu TCP/IP?	
Provedli jste nejnovější opravy PTF?	
Jestliže tunel VPN prochází ochrannými bariérami (firewall) nebo směrovači, které používají filtrování IP paketů, podporují filtrovací pravidla ochranných bariér a směrovačů protokoly AH a ESP?	
Jsou ochranné bariéry nebo směrovače konfigurovány tak, že povolují protokoly AH a ESP?	
Jsou ochranné bariéry konfigurovány tak, že umožňují směrování pomocí IP?	

Informace potřebné pro konfiguraci manuálního připojení VPN	Odpovědi
Jaký typ připojení vytváříte? • Hostitelský systém - hostitelský systém • Hostitelský systém - komunikační brána • Komunikační brána - hostitelský systém • Komunikační brána - komunikační brána	
Jak připojení pojmenujete?	
Jaký je identifikátor lokálního koncového systému?	
Jaký je identifikátor vzdáleného koncového systému?	
Jaký je identifikátor lokálního datového koncového systému?	
Jaký je identifikátor vzdáleného datového koncového systému?	
Jaký typ provozu povolíte pro toto připojení (lokální port, vzdálený port a protokol)?	
Požadujete pro toto připojení převod adres? Další informace najdete v části Převod síťových adres pro VPN.	
Budete používat režim tunelu nebo režim přenosu?	
Který protokol IPSec bude připojení používat (AH, ESP nebo AH spolu s ESP)? Další informace najdete v části IPSec (IP Security).	
Který autentizační algoritmus bude připojení používat (HMAC-MD5 nebo HMAC-SHA)?	
Který šifrovací algoritmus bude připojení používat (DES-CBC nebo 3DES-CBC)? **Poznámka:** Šifrovací algoritmus zadejte pouze tehdy, pokud jste vybrali jako protokol IPSec protokol ESP.	
Jaký je příchozí klíč AH? Pokud používáte MD5, je klíč 16bajtový hexadecimální řetězec. Pokud používáte SHA, je klíč 20bajtový hexadecimální řetězec. Příchozí klíč se musí přesně shodovat s odchozím klíčem vzdáleného serveru.	

Informace potřebné pro konfiguraci manuálního připojení VPN	Odpovědi
Jaký je odchozí klíč AH? Pokud používáte MD5, je klíč 16bajtový hexadecimální řetězec. Pokud používáte SHA, je klíč 20bajtový hexadecimální řetězec. Odchozí klíč se musí přesně shodovat s příchozím klíčem vzdáleného serveru.	
Jaký je příchozí klíč ESP? Pokud používáte DES, je klíč 8bajtový hexadecimální řetězec. Pokud používáte 3DES, je klíč 24bajtový hexadecimální řetězec. Příchozí klíč se musí přesně shodovat s odchozím klíčem vzdáleného serveru.	
Jaký je odchozí klíč ESP? Pokud používáte DES, je klíč 8bajtový hexadecimální řetězec. Pokud používáte 3DES, je klíč 24bajtový hexadecimální řetězec. Odchozí klíč se musí přesně shodovat s příchozím klíčem vzdáleného serveru.	
Jaký je příchozí index SPI (Security Policy Index)? Příchozí index SPI je 4bajtový hexadecimální řetězec, ve kterém je první bajt nastaven na hodnotu 00. Příchozí index SPI se musí přesně shodovat s odchozím indexem SPI vzdáleného serveru.	
Jaký je odchozí index SPI? Odchozí index SPI je 4bajtový hexadecimální řetězec. Odchozí index SPI se musí přesně shodovat s příchozím indexem SPI vzdáleného serveru.	

Konfigurace VPN

Rozhraní VPN umožňuje několik různých způsobů konfigurace připojení VPN. Pokračujte v čtení, pomůže vám to při rozhodování o tom, který typ připojení máte konfigurovat a jak.

Jaký typ připojení konfigurovat
Dynamické připojení dynamicky generuje a vyjednává klíče, které zabezpečují ochranu aktivního připojení pomocí protokolu IKE (Internet Key Exchange). Dynamická připojení poskytují mimořádnou úroveň zabezpečení ochrany dat, která jimi procházejí, protože se klíče mění automaticky v pravidelných intervalech. V důsledku toho je méně pravděpodobné, že by útočník zachytil klíč, měl dostatek času ho rozluštit a použít k vychýlení nebo zaznamenání provozu, který je tímto klíčem chráněn.

Manuální (strana 36) připojení ale neposkytuje podporu vyjednávání IKE a v důsledku toho ani automatické správě klíčů. Oba konce připojení dále vyžadují konfiguraci několika atributů, které se musejí přesně shodovat. Manuální připojení používají statické klíče, které nelze obnovit ani měnit, dokud je připojení aktivní. Manuální připojení musíte ukončit, chcete-li změnit jeho asociovaný klíč. Pokud toto považujete za bezpečnostní riziko, můžete místo manuálního připojení vytvořit dynamické.

Jak konfigurovat dynamické připojení VPN
VPN je ve skutečnosti skupina konfiguračních objektů, které určují charakteristiku připojení. Dynamické připojení do VPN vyžaduje, aby každý z těchto objektů řádně pracoval. Další informace o tom, jak konfigurovat jednotlivé konfigurační objekty, najdete pod níže uvedenými odkazy:

> **Rada:**
> **Konfigurace připojení VPN pomocí průvodce novým připojením**
> Všechna dynamická připojení můžete obecně vytvářet pomocí průvodce připojením. Průvodce automaticky vytvoří každý z konfiguračních objektů, které VPN k řádnému fungování vyžaduje, včetně pravidel paketů. Pokud zadáte, že chcete, aby průvodce aktivoval pravidla paketů VPN, můžete přejít níže ke kroku 6, *Spustit připojení*. Jinak musíte poté, co průvodce dokončí konfigurování připojení VPN, aktivovat pravidla paketů a potom spustit připojení.

Pokud nechcete při konfigurování dynamického připojení VPN používat průvodce, dokončete konfiguraci takto:

1. **Konfigurace zásad zabezpečení VPN**
   Pro všechna dynamická připojení musíte definovat zásady zabezpečení VPN. Zásada IKE (Internet Key Exchange) a zásada pro práci s daty předpisují, jak IKE chrání vyjednávání své fáze 1 a fáze 2.
2. **Konfigurace zabezpečených připojení**
   Když pro připojení definujete zásady zabezpečení, musíte pak konfigurovat zabezpečené připojení. U dynamických připojení obsahuje objekt zabezpečeného připojení skupinu s dynamicky přiřazeným klíčem a připojení s dynamicky přiřazeným klíčem. **Skupina s dynamicky přiřazeným klíčem** určuje společnou charakteristiku jednoho nebo více připojení VPN. **Připojení s dynamicky přiřazeným klíčem** definuje charakteristiku jednotlivých datových připojení mezi dvěma koncovými systémy. Skupina s dynamicky přiřazeným klíčem obsahuje připojení s dynamicky přiřazeným klíčem.

   Poznámka: Následující dva kroky, *Konfigurace pravidel paketů* a *Definice rozhraní pro pravidla*, musíte provést pouze tehdy, pokud jste v rozhraní VPN na straně **Skupina s dynamicky přiřazeným klíčem - Připojení** vybrali volbu **Filtrovací pravidla zásad budou definována v Pravidlech paketů**. Jinak budou tato pravidla vytvořena jako součást konfigurací VPN a budou uplatněna na zadané rozhraní.

   Doporučuje se, aby filtrovací pravidla zásad byla vždy vytvářena rozhraním VPN. K tomu stačí vybrat volbu **Vytvořit následující filtr zásad pro tuto skupinu** na straně **Skupina s dynamicky přiřazeným klíčem - Připojení**.
3. **Konfigurace pravidel paketů**
   Po dokončení konfigurace VPN musíte vytvořit a uplatnit filtrovací pravidla, která povolí provoz tímto připojením. Pravidla **pre-IPSec** připojení VPN povolují veškerý provoz IKE v zadaných rozhraních, takže IKE může vyjednávat připojení. **Filtrovací pravidlo zásad** určuje, které adresy, protokoly a porty mohou používat novou asociovanou skupinu s dynamicky přiřazeným klíčem.

   Provádíte-li migraci buď z verze V4R4, nebo z verze V4R5 a chcete v aktuální verzi nadále používat připojení VPN a filtry zásad, prostudujte si téma *Migrace filtrů zásad na aktuální vydání*. Staré a nové filtry zásad mohou spolupracovat podle vašeho přání.
4. **Definice rozhraní pro pravidla**
   Až dokončíte konfiguraci pravidel paketů a libovolných jiných pravidel, která potřebujete, chcete-li povolit připojení VPN, musíte definovat rozhraní, na které tato pravidla uplatníte.
5. **Aktivace pravidel paketů**
   Až dokončíte definici rozhraní pro pravidla paketů, musíte ještě před spuštěním připojení tato pravidla aktivovat.
6. **Spuštění připojení**
   Až dokončíte tento úkol, budou připojení spuštěna.

Jak konfigurovat manuální připojení VPN

Jak naznačuje jméno, v manuálním připojení musíte všechny vlastnosti VPN konfigurovat ručně včetně příchozích a odchozích klíčů. Další informace o tom, jak konfigurovat manuální připojení, najdete pod níže uvedenými odkazy:

1. **Konfigurace manuálních připojení**
   Manuální připojení definují charakteristiku připojení včetně protokolů zabezpečení a koncových systémů připojení a dat.

   Poznámka: Následující dva kroky, *Konfigurace filtrovacích pravidel paketů* a *Definice rozhraní pro pravidla*, musíte provést pouze tehdy, pokud jste v rozhraní VPN na straně **Manuální připojení - Připojení** vybrali volbu **Filtrovací pravidla zásad budou definována v Pravidlech paketů**. Jinak budou tato pravidla vytvořena jako součást konfigurací VPN.

   Doporučuje se, aby filtrovací pravidla zásad byla vždy vytvářena rozhraním VPN. K tomu stačí vybrat volbu **Generovat filtry zásad, které vyhovují datovým koncovým systémům** na straně **Manuální připojení - Připojení**.
2. **Konfigurace filtrovacích pravidel zásad**
   Po dokončení konfigurace atributů manuálního připojení musíte vytvořit a uplatnit filtrovací pravidlo zásad, které povolí provoz tímto připojením. **Filtrovací pravidlo zásad** určuje, které adresy, protokoly a porty mohou asociované připojení používat.
3. **Definice rozhraní pro pravidla**
   Až dokončíte konfiguraci pravidel paketů a libovolných jiných pravidel, která potřebujete, chcete-li povolit připojení VPN, musíte definovat rozhraní, na které tato pravidla uplatníte.

4. **Aktivace pravidel paketů**
   Až dokončíte definici rozhraní pro pravidla paketů, musíte ještě před spuštěním připojení tato pravidla aktivovat.
5. **Spuštění připojení**
   Až dokončíte tento úkol, budou lokálně iniciovaná připojení spuštěna.

Konfigurace připojení VPN pomocí průvodce novým připojením

Průvodce novým připojením vám umožňuje vytvořit VPN mezi libovolnou kombinací hostitelských systémů a komunikačních bran, například hostitelský systém - hostitelský systém, komunikační brána - hostitelský systém, hostitelský systém - komunikační brána a komunikační brána - komunikační brána.

Průvodce automaticky vytvoří každý z konfiguračních objektů, které VPN k řádnému fungování vyžaduje, včetně pravidel paketů. Chcete-li ale do VPN přidat funkci, například žurnálování nebo převod síťových adres pro VPN (VPN NAT), budete možná chtít upřesnit konfiguraci VPN pomocí listů vlastností příslušných skupin a připojení s dynamicky přiřazeným klíčem. K tomu musíte nejprve ukončit připojení, je-li aktivní. Potom klepněte pravým tlačítkem na skupinu či připojení s dynamicky přiřazeným klíčem a vyberte **Vlastnosti**.

Než začnete, dokončete práci s poradcem při plánování VPN. Poradce poskytuje prostředky pro shromažďování důležitých informací, které budete potřebovat při vytváření VPN.

Chcete-li vytvořit VPN pomocí průvodce připojením, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Nové připojení**. Tím spustíte průvodce.
3. Dokončete průvodce a vytvořte základní připojení VPN. Potřebujete-li pomoc, klepněte na tlačítko **Nápověda**.

Konfigurace zásad zabezpečení VPN

Až určíte, jak budete VPN používat, musíte definovat zásady zabezpečení VPN. Patří mezi ně:

- **Konfigurace zásady IKE (Internet Key Exchange)**
  Zásada IKE určuje, jakou úroveň autentizace a šifrování používá IKE při vyjednáváních fáze 1. Fáze 1 IKE vytvoří klíče, které chrání zprávy postupující do následujících vyjednávání fáze 2. Když vytváříte manuální připojení, nemusíte zásadu IKE definovat. Vytváříte-li VPN pomocí průvodce novým připojením, průvodce může zásadu IKE vytvořit za vás.
- **Konfigurace zásad pro práci s daty**
  Zásada pro práci s daty určuje, jaká úroveň autentizace nebo šifrování chrání data při postupu VPN. Komunikační systémy se na těchto atributech dohodnou při vyjednáváních fáze 2 protokolu IKE (Internet Key Exchange). Když vytváříte manuální připojení, nemusíte zásadu pro práci s daty definovat. Vytváříte-li VPN pomocí průvodce novým připojením, průvodce může zásadu pro práci s daty vytvořit za vás.

Až dokončíte konfiguraci zásad zabezpečení VPN, musíte konfigurovat zabezpečená připojení.

Konfigurace zásady IKE (Internet Key Exchange)

Zásada IKE určuje, jakou úroveň autentizace nebo šifrování používá IKE při vyjednáváních fáze 1. Fáze 1 IKE vytvoří klíče, které chrání zprávy postupující do následujících vyjednávání fáze 2. VPN používá při autentizaci vyjednávání fáze 1 buď zásadu podpisu RSA, nebo předem nasdílené klíče. Chcete-li při autentizaci klíčových serverů používat certifikáty, musíte je nejprve konfigurovat pomocí produktu DCM (Digital Certificate Manager) (5722-SS1 volba 34). Zásada IKE také určuje, který vzdálený klíčový server bude tuto zásadu používat.

Chcete-li definovat zásadu IKE nebo změnit stávající zásadu, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zásady zabezpečení IP**.

2. Chcete-li vytvořit novou zásadu, klepněte pravým tlačítkem na **Zásady IKE (Internet Key Exchange)** a vyberte **Nová zásada IKE (Internet Key Exchange Policy)**. Chcete-li provádět změny stávající zásady IKE, klepněte na **Zásady IKE (Internet Key Exchange)** v levém podokně, a potom v pravém podokně klepněte pravým tlačítkem na zásadu, kterou chcete změnit, a vyberte **Vlastnosti**.
3. Vyplňte všechny listy vlastností. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Klepnutím na tlačítko **OK** uložte provedené změny.

Poznámka: Kdykoli je při autentizaci použit předem nasdílený klíč, doporučuje se používat vyjednávání v hlavním režimu. Tato vyjednávání poskytují lépe zabezpečenou výměnu. Pokud musíte použít předem nasdílený klíč a vyjednávání v agresívním režimu, vyberte si záhadná hesla, která bude obtížné zachytit při napadení, která snímají slovník. Také se doporučuje, abyste hesla pravidelně měnili. Podrobnější informace najdete v nápovědě produktu iSeries Navigator.

Konfigurace zásad pro práci s daty

Zásada pro práci s daty určuje, jaká úroveň autentizace nebo šifrování chrání data při postupu sítí VPN. Komunikační systémy se na těchto atributech dohodnou při vyjednáváních fáze 2 protokolu IKE (Internet Key Exchange).

Chcete-li definovat zásadu pro práci s daty nebo změnit stávající zásadu, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zásady zabezpečení IP**.
2. Chcete-li vytvořit novou zásadu pro práci s daty, klepněte pravým tlačítkem na **Zásady pro práci s daty** a vyberte **Nová zásada pro práci s daty**. Chcete-li provádět změny stávající zásady pro práci s daty, klepněte na **Zásady pro práci s daty** (v levém podokně) a potom klepněte pravým tlačítkem na zásadu, kterou chcete změnit, a vyberte **Vlastnosti**.
3. Vyplňte všechny listy vlastností. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Klepnutím na tlačítko **OK** uložte provedené změny.

Konfigurace zabezpečeného připojení VPN

Až dokončíte konfiguraci zásad zabezpečení, musíte konfigurovat zabezpečené připojení. U dynamických připojení obsahuje objekt zabezpečeného připojení skupinu s dynamicky přiřazeným klíčem a připojení s dynamicky přiřazeným klíčem.

Skupina s dynamicky přiřazeným klíčem určuje společnou charakteristiku jednoho nebo více připojení VPN. Konfigurování skupiny s dynamicky přiřazeným klíčem dovoluje použít pro každé připojení ve skupině stejné zásady, ale odlišné datové koncové systémy. Skupiny s dynamicky přiřazeným klíčem také umožňují úspěšně vyjednávat se vzdálenými iniciátory, když datové koncové systémy navrhované vzdáleným systémem nejsou přesně známy předem. Informace zásad ve skupině s dynamicky přiřazeným klíčem jsou asociovány s filtrovacím pravidlem zásad s typem akce IPSEC. Pokud specifické datové koncové systémy nabídnuté vzdáleným iniciátorem jsou v rozsahu určeném filtrovacím pravidlem IPSEC, mohou být podřízeny zásadě definované ve skupině s dynamicky přiřazeným klíčem.

Připojení s dynamicky přiřazeným klíčem definuje charakteristiku jednotlivých datových připojení mezi dvěma koncovými systémy. Připojení s dynamicky přiřazeným klíčem existuje ve skupině s dynamicky přiřazeným klíčem. Když dokončíte konfiguraci skupiny s dynamicky přiřazeným klíčem a popíšete, které zásady připojení ve skupině používat, musíte vytvořit jednotlivá připojení s dynamicky přiřazeným klíčem pro připojení iniciovaná lokálně.

Chcete-li konfigurovat objekt zabezpečeného připojení, proveďte tyto úkoly:

Část 1: Konfigurace skupiny s dynamicky přiřazeným klíčem:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepněte pravým tlačítkem na **Podle skupin** a vyberte **Nová skupina s dynamicky přiřazeným klíčem**.
3. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Klepnutím na tlačítko **OK** uložte provedené změny.

Část 2: Konfigurace připojení s dynamicky přiřazeným klíčem:

1. V produktu iSeries Navigator rozbalte svůj server **—> Síť —> Zásady pro práci s IP —> VPN (Virtual Private Networking) —> Zabezpečená připojení —> Podle skupin**.
2. V levém podokně okna produktu iSeries Navigator klepnutí pravým tlačítkem na skupinu s dynamicky přiřazeným klíčem vytvořenou v části 1 a vyberte **Nové připojení s dynamicky přiřazeným klíčem**.
3. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Klepnutím na tlačítko **OK** uložte provedené změny.

Po provedení těchto kroků musíte aktivovat pravidla paketů, která toto připojení vyžaduje, aby mohlo řádně fungovat.

Poznámka: Ve většině případů je vhodné dovolit, aby rozhraní VPN automaticky generovalo pravidla paketů pomocí volby **Generovat následující filtry zásad pro tuto skupinu** na straně **Skupina s dynamicky přiřazeným klíčem - Připojení**. Pokud ale vyberete volbu **Filtrovací pravidlo zásad bude definováno v Pravidlech paketů**, musíte pak konfigurovat pravidla paketů VPN pomocí editoru pravidel paketů a potom je aktivovat.

Konfigurace manuálních připojení VPN

Jak naznačuje jméno, v manuálním připojení musíte všechny vlastnosti VPN konfigurovat ručně. Oba konce připojení dále vyžadují konfiguraci několika prvků, které se musejí *přesně* shodovat. Například příchozí klíče se musejí shodovat s odchozími klíči vzdáleného systému, jinak připojení selže.

Manuální připojení používají statické klíče, které se nelze obnovit ani měnit, dokud je připojení aktivní. Chcete-li změnit asociovaný klíč manuálního připojení, musíte toto připojení ukončit. Pokud toto považujete za bezpečnostní riziko a oba konce připojení podporují protokol IKE (Internet Key Exchange), můžete místo manuálního připojení vytvořit dynamické.

Chcete-li definovat vlastnosti manuálního připojení, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepněte pravým tlačítkem na **Všichni uživatelé** a vyberte **Nové manuální připojení**.
3. Vyplňte všechny listy vlastností. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Klepnutím na tlačítko **OK** uložte provedené změny.

Poznámka: Ve většině případů je vhodné dovolit, aby rozhraní VPN automaticky generovalo pravidla paketů pomocí volby **Generovat filtr zásad odpovídající datovým koncovým systémům** na straně **Manuální připojení - Připojení**. Vyberete-li však volbu **Filtrovací pravidlo zásad bude definováno v Pravidlech paketů**, musíte pak konfigurovat filtrovací pravidla zásad ručně a potom je aktivovat.

Konfigurace pravidel paketů VPN

Vytváříte-li připojení poprvé, dovolte, aby pravidla paketů byla automaticky generována pomocí VPN. Můžete to provést tak, že při konfiguraci připojení VPN použijete buď průvodce novým připojením, nebo strany vlastností VPN.

Pokud jste se rozhodli použít při vytváření pravidel paketů VPN editor Pravidel paketů v produktu iSeries(TM) Navigator, vytvořte také všechna další pravidla tímto způsobem. Pokud byla filtrovací pravidla zásad vygenerována pomocí VPN, vytvořte také všechna další pravidla tímto způsobem.

Připojení VPN vyžadují obecně dva typy filtrovacích pravidel: filtrovací pravidla pre-IPSec a filtrovací pravidla zásad. Chcete-li zjistit, jak lze tato pravidla konfigurovat pomocí editoru pravidel paketů v produktu iSeries Navigator, prostudujte níže uvedená témata. Informace o dalších možnostech VPN a filtrování najdete v tématu Koncepce VPN v části *VPN a IP filtrování*.

- **Pravidla pre-IPSec**
  Pravidla pre-IPSec jsou libovolná pravidla v systému, která předcházejí pravidla s typem akce IPSEC. Toto téma se věnuje pouze pravidlům pre-IPSec, u kterých VPN vyžaduje, aby fungovala správně. V tomto případě jsou pravidla pre-IPSec dvojicí pravidel, které umožňují zpracování IKE přes připojení. IKE dovoluje generování a vyjednávání dynamického klíče pro připojení. Další pravidla pre-IPSec můžete přidat v závislosti na konkrétním síťovém prostředí a strategii zabezpečení.

  Poznámka: Tento typ pravidla pre-IPSec můžete konfigurovat, až když už máte ostatní pravidla, která povolují IKE pro určité systémy. Nejsou-li v systému žádná filtrovací pravidla napsaná speciálně pro povolení provozu IKE, je provoz IKE implicitně povolen.
- **Filtrovací pravidlo zásad**
  Filtrovací pravidlo zásad definuje provoz, který může používat VPN, a zásady ochrany dat, které mají být na tento provoz uplatněny.

Než začnete
Přidáte-li k nějakému rozhraní filtrovací pravidla, systém k tomuto rozhraní automaticky přidá předvolené pravidlo DENY. To znamená, že každý provoz, který není výslovně povolen, je odepřen. Toto pravidlo nelze zobrazit ani změnit. Výsledkem může být, že provoz, který dříve perfektně fungoval, selže po aktivaci filtrovacích pravidel VPN. Chcete-li v rozhraní povolit jiný provoz než VPN, musíte přidat explicitní pravidla PERMIT.

Po dokončení konfigurace příslušných filtrovacích pravidel musíte definovat rozhraní, na které budou uplatněna a potom je aktivovat.

Je velmi důležité, abyste filtrovací pravidla konfigurovali řádně. Jinak mohou zablokovat veškerý příchozí i odchozí IP provoz na serveru iSeries. Zahrnuje to i připojení k produktu iSeries Navigator, které používáte při konfiguraci filtrovacích pravidel.

Pokud filtrovací pravidla nepovolují provoz produktu iSeries Navigator, nemůže tento produkt komunikovat se serverem iSeries. Pokud dojde k této situaci, musíte se přihlásit k serveru iSeries pomocí rozhraní, které ještě má připojitelnost, například z konzole Operations Console. Příkazem RMVTCPTBL můžete ze systému odstranit všechny filtry. Tento příkaz také ukončí práci serverů *VPN a pak je restartuje. Potom proveďte konfiguraci filtrů a znovu je aktivujte.

Konfigurace filtrovacího pravidla pre-IPSec

Upozornění: Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby filtrovací pravidla zásad byla automaticky generována VPN.

Dvojice serverů IKE (Internet Key Exchange) dynamicky vyjednává a obnovuje klíče. Připojení IKE používá známý port s číslem 500. Chcete-li, aby protokol IKE pracoval správně, musíte pro tento IP provoz povolit datagramy UDP přes port 500. K tomu stačí vytvořit dvojici filtrovacích pravidel, jedno pro příchozí a druhé pro odchozí provoz. Připojení pak může dynamicky vyjednávat klíče, které chrání připojení.

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketů** a vyberte **Editor pravidel**. Otevře se editor Pravidel paketů a umožní vám vytvořit nebo upravit filtr a pravidla pro převod síťových adres (NAT) pro server iSeries.
3. V okně Vítejte vyberte **Vytvořit nový soubor pravidel paketů** a klepněte na tlačítko **OK**.
4. V editoru pravidel paketů vyberte **Vložit —> Filtr**.
5. Na straně **Obecné** zadejte jméno filtrovacího pravidla VPN. Doporučuje se vytvořit alespoň tři různé sady: jednu pro filtrovací pravidla pre-IPSec, jednu pro filtrovací pravidla zásad a jednu pro různá filtrovací pravidla PERMIT a DENY. Jméno sady, která obsahuje filtrovací pravidla pre-IPSec, by mělo obsahovat předponu *preipsec*, například preipsecfilters.
6. V poli **Akce** vyberte v rozbalovacím seznamu **PERMIT**.

7. V poli **Směr** vyberte v rozbalovacím seznamu **OUTBOUND**.
8. V poli **Jméno zdrojové adresy** vyberte v rozbalovacím seznamu znak **=** a potom do druhého pole zadejte IP adresu lokálního klíčového serveru. IP adresu lokálního klíčového serveru jste zadali v zásadě IKE.
9. V poli **Jméno cílové adresy** vyberte v rozbalovacím seznamu znak **=** a potom do druhého pole zadejte IP adresu vzdáleného klíčového serveru. IP adresu vzdáleného klíčového serveru jste také zadali v zásadě IKE.
10. Na straně **Služby** vyberte **Služba**. Zpřístupní se tak pole **Protokol**, **Zdrojový port** a **Cílový port**.
11. V poli **Protokol** vyberte v rozbalovacím seznamu **UDP**.
12. V prvním poli vyberte pro **Zdrojový port** znak **=** a v druhém poli zadejte hodnotu 500.
13. Opakujte předchozí krok pro **Cílový port**.
14. Klepněte na tlačítko **OK**.
15. Opakujte tento postup při konfiguraci filtru INBOUND. Použijte stejné jméno sady a příslušné adresy.

Poznámka: Méně bezpečnou, ale snazší možností povolení provozu IKE tímto připojením je konfigurovat pouze jeden filtr pre-IPSec a použít v polích **Směr**, **Zdrojová adresa** a **Cílová adresa** zástupné znaky (*).

Dalším krokem je konfigurace filtrovacích pravidel zásad . Určí se v něm, který IP provoz je připojením do VPN chráněn.

Konfigurace filtrovacích pravidel zásad

Upozornění: Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby filtrovací pravidla zásad byla automaticky generována VPN.

Filtrovací pravidlo zásad (tj. pravidlo, ve kterém action=IPSEC) určuje, které adresy, protokoly a porty může VPN používat. Určuje také zásadu, která bude na provoz v připojení VPN uplatněna. Chcete-li konfigurovat filtrovací pravidlo zásad, postupujte takto:

Poznámka: Pokud jste právě konfigurovali pravidlo pre-IPSec (pouze pro dynamická připojení), bude editor Pravidel paketů ještě otevřený. Přejděte ke kroku 4.

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketů** a vyberte **Editor pravidel**. Otevře se editor Pravidel paketů a umožní vám vytvořit nebo upravit filtr a pravidla pro převod síťových adres (NAT) pro server iSeries.
3. V okně Vítejte vyberte **Vytvořit nový soubor pravidel paketů** a klepněte na tlačítko **OK**.
4. V editoru pravidel paketů vyberte **Vložit —> Filtr**.
5. Na straně **Obecné** zadejte jméno filtrovacího pravidla VPN. Doporučuje se vytvořit alespoň tři různé sady: jednu pro filtrovací pravidla pre-IPSec, jednu pro filtrovací pravidla zásad a jednu pro různá filtrovací pravidla PERMIT a DENY, například policyfilters.
6. V poli **Akce** vyberte v rozbalovacím seznamu **IPSEC**. Pole **Směr** nabývá předem stanovené hodnoty OUTBOUND, kterou nelze měnit. Přesto je toto pole ve skutečnosti dvousměrné. Zobrazená hodnota OUTBOUND objasňuje sémantiku vstupních hodnot. Například zdrojové hodnoty jsou lokální a cílové hodnoty jsou vzdálené.
7. V poli **Jméno zdrojové adresy** vyberte v rozbalovacím seznamu znak **=** a potom do druhého pole zadejte IP adresu lokálního datového koncového systému. Můžete také zadat rozsah IP adres a masku podsítě, když je nejprve zadáte pomocí funkce **Definovat adresy**.
8. V poli **Jméno cílového adresy** vyberte v rozbalovacím seznamu znak **=** a potom do druhého pole zadejte IP adresu vzdáleného datového koncového systému. Můžete také zadat rozsah IP adres a masku podsítě, když je nejprve zadáte pomocí funkce **Definovat adresy**.
9. V poli **Zápis do žurnálu** zadejte požadovanou úroveň žurnálování.
10. V poli **Jméno připojení** vyberte definici připojení, na které budou tato filtrovací pravidla uplatněna.
11. (volitelné) Zadejte popis.
12. Na straně **Služby** vyberte **Služba**. Zpřístupní se tak pole **Protokol**, **Zdrojový port** a **Cílový port**.

13. V polích **Protokol**, **Zdrojový port** a **Cílový port** vyberte hodnoty vhodné pro tento provoz. Z rozbalovacího seznamu můžete také vybrat hvězdičku (*). Tím každému protokolu umožníte použít pro VPN libovolný port.
14. Klepněte na tlačítko **OK**.

Dalším krokem je určení rozhraní, na které budou tato filtrovací pravidla uplatněna.

Poznámka: Přidáte-li k nějakému rozhraní filtrovací pravidla, systém k tomuto rozhraní automaticky přidá předvolené pravidlo DENY. To znamená, že každý provoz, který není výslovně povolen, je odepřen. Toto pravidlo nelze zobrazit ani změnit. Výsledkem může být, že připojení, která dříve perfektně fungovala, selžou po aktivaci pravidel paketů VPN. Chcete-li v rozhraní povolit jiný provoz než VPN, musíte přidat explicitní pravidla PERMIT.

Definice rozhraní pro filtrovací pravidla VPN

Až dokončíte konfiguraci pravidel paketů VPN a libovolných jiných pravidel, která potřebujete, chcete-li povolit připojení VPN, musíte definovat rozhraní, na které tato pravidla uplatníte.

Chcete-li definovat rozhraní, na které uplatníte filtrovací pravidla VPN, postupujte takto:

Poznámka: Pokud jste právě konfigurovali pravidlo VPN, bude rozhraní pravidel paketů ještě otevřené. Přejděte ke kroku 4.

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketu** a vyberte **Editor pravidel**. Otevře se editor Pravidel paketů a umožní vám vytvořit nebo upravit filtr a pravidla pro převod síťových adres (NAT) pro server iSeries.
3. V okně Vítejte vyberte **Vytvořit nový soubor pravidel paketů** a klepněte na tlačítko **OK**.
4. V editoru pravidel paketů vyberte **Vložit —> Filtrovací rozhraní**.
5. Na straně **Obecné** vyberte **Jméno linky** a potom vyberte z rozbalovacího seznamu popis linky, na kterou budou uplatněna pravidla paketů.
6. (volitelné) Zadejte popis.
7. Každé jméno sady právě konfigurovaných filtrů přidejte klepnutím na tlačítko **Přidat** na straně **Sady filtrů**.
8. Klepněte na tlačítko **OK**.
9. Uložte soubor s pravidly. Soubor bude uložený do integrovaného systému souborů na serveru iSeries s příponou .i3p.
   Poznámka: Neukládejte soubor do tohoto adresáře:
   ```
   /QIBM/UserData/OS400/TCPIP/RULEGEN
   ```
   Tento adresář je pouze pro systémové použití. Pokud budete potřebovat deaktivovat pravidla paketů pomocí příkazu RMVTCPTBL *ALL, vymaže tento příkaz všechny soubory v tomto adresáři.

Až dokončíte definici rozhraní pro filtrovací pravidla, musíte ještě před spuštěním připojení VPN tato pravidla aktivovat.

Aktivace pravidel paketů VPN

Před spuštěním vlastních připojení VPN musíte aktivovat pravidla paketů VPN. Tato pravidla nelze aktivovat ani deaktivovat, pokud jsou v systému spuštěna připojení VPN. Před aktivací filtrovacích pravidel VPN zajistěte, aby žádné připojení, které je s ním asociované, nebylo neaktivní.

Pokud jste svá připojení VPN vytvářeli pomocí Průvodce novým připojením, můžete zvolit, zda mají být přiřazená pravidla aktivována automaticky. Uvědomte si však, že pokud jsou aktivní jiná pravidla paketů v libovolném rozhraní, která jste zadali, tato filtrovací pravidla zásad připojení VPN je nahradí.

Chcete-li zvolit aktivaci pravidel generovaných VPN pomocí editoru pravidel paketů, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketů** a vyberte **Aktivovat**. Otevře se dialog **Aktivovat pravidla paketů**.

3. Vyberte, zda chcete aktivovat pouze pravidla generovaná VPN, pouze vybraný soubor, nebo obojí. Mohli byste vybrat posledně jmenovanou možnost, máte-li mnoho různých pravidel pro povolení a odepření přístupu, která chcete kromě pravidel generovaných VPN v rozhraní používat.
4. Vyberte rozhraní, ve kterém chcete pravidla aktivovat. Můžete si vybrat, zda chcete aktivovat v zadaném rozhraní, v identifikátoru PPP, ve všech rozhraních, nebo ve všech identifikátorech PPP.
5. Klepnutím na tlačítko **OK** v dialogu potvrdíte, že chcete pravidla ověřit a aktivovat ve vybraných rozhraních. Systém pak pravidla zkontroluje a ohlásí případné syntaktické a sémantické chyby v okně zprávy v dolní části okna editoru. Chcete-li zjistit, ke kterému souboru a číslu řádku jsou chybové zprávy přiřazeny, klepněte pravým tlačítkem na chybu a vyberte příkaz **Přejít na řádek**. Chyba bude v souboru zvýrazněna.

Po aktivaci filtrovacích pravidel můžete spustit připojení VPN.

Spuštění připojení VPN

V těchto pokynech předpokládáme, že máte řádně konfigurované připojení VPN. Chcete-li spustit připojení VPN, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Není-li server VPN spuštěn, klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**. Tím se server VPN spustí.
3. Přesvědčte se, že pravidla paketů jsou aktivována.
4. Rozbalte **VPN (Virtual Private Networking)—>Zabezpečená připojení**.
5. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
6. Klepněte pravým tlačítkem na připojení, které chcete spustit, a vyberte **Spustit**. Chcete-li spustit několik připojení, vyberte každé z nich jednotlivě, klepněte pravým tlačítkem a vyberte **Spustit**.

Správa VPN

Při provádění úkolů správy používejte rozhraní VPN v produktu iSeries(TM) Navigator. Mezi tyto úkoly patří:

- **Spuštění připojení VPN**
  Až dokončíte tento úkol, budou lokálně iniciovaná připojení spuštěna.
- **Nastavení předvolených atributů pro připojení**
  Předvolené hodnoty naplní dialogová okna, ve kterých vytváříte nové zásady a připojení. Předvolby můžete nastavit pro úrovně zabezpečení, správu relací klíčů, dobu trvání klíčů a dobu trvání připojení.
- **Obnova připojení v chybovém stavu**
  Obnovou připojení v chybovém stavu vrátíte tato připojení do stavu Nečinný.
- **Prohlížení informací o chybách**
  Až dokončíte tento úkol, můžete snáze určit, proč je připojení chybné.
- **Prohlížení atributů aktivních připojení**
  Až dokončíte tento úkol, můžete zkontrolovat stav a ostatní atributy aktivních připojení.
- **Použití trasování serveru VPN**
  Trasování serveru VPN vám umožňuje konfigurovat, spustit, ukončit a prohlížet trasování Správce připojení VPN a Správce klíčů VPN. Je to podobné jako použití příkazu TRCTCPAPP *VPN ze znakově orientovaného rozhraní, s výjimkou toho, že trasování můžete prohlížet, když je připojení aktivní.
- **Prohlížení protokolů úloh serveru VPN**
  Dodržujte tyto pokyny, chcete-li prohlížet protokoly úloh pro servery Správce klíčů VPN a Správce připojení VPN.
- **Ukončení připojení**
  Až dokončíte tento úkol, budou aktivní připojení ukončena.
- **Prohlížení atributů Přidružení zabezpečení (SA)**
  Až dokončíte tento úkol, budou zobrazeny atributy přidružení zabezpečení, které jsou asociovány s aktivním připojením.

- **Výmaz konfiguračních objektů VPN**
  Dříve než vymažete konfigurační objekt VPN z databáze zásad VPN, ujistěte se, že jste porozuměli tomu, jak to ovlivní ostatní připojení VPN a skupiny připojení.

Nastavení předvolených atributů pro připojení

Když poprvé vytvoříte nové objekty VPN, naplní předvolené hodnoty zabezpečení mnoho různých polí.

Chcete-li nastavit předvolené hodnoty zabezpečení, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—>Síť —>Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Předvolby**.
3. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
4. Po vyplnění všech listů vlastností klepněte na tlačítko **OK**.

Obnova připojení v chybovém stavu

Chcete-li obnovit připojení, které je v chybovém stavu, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepněte pravým tlačítkem na připojení, které chcete obnovit, a vyberte **Vynulovat**. Tím bude nastaven nečinný stav připojení. Chcete-li obnovit několik připojení, která jsou v chybovém stavu, musíte vybrat každé jednotlivé připojení, klepnout na ně pravým tlačítkem a vybrat **Vynulovat**.

Prohlížení informací o chybách

Chcete-li prohlížet informace o chybných připojeních, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepněte pravým tlačítkem na chybné připojení, které chcete prohlížet, a vyberte **Informace o chybě**.

Prohlížení atributů aktivních připojení

Chcete-li prohlížet aktuální atributy aktivního připojení nebo připojení na žádost, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepnutím pravým tlačítkem na aktivní připojení nebo na připojení na žádost, které chcete prohlížet, a vyberte **Vlastnosti**.
4. Chcete-li prohlížet atributy tohoto připojení, přejděte na stranu **Aktuální atributy**.

V okně produktu iSeries Navigator můžete prohlížet atributy všech připojení. Standardně jsou zobrazeny pouze atributy Stav, Popis a Typ připojení. Chcete-li zobrazit i jiné údaje, postupujte takto:

1. V produktu iSeries Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. V menu **Objekty** vyberte příkaz **Sloupce**. Otevře se dialog, ve kterém můžete vybrat atributy, které budou zobrazeny v okně iSeries Navigator.

Uvědomte si, že když změníte zobrazení sloupců v okně iSeries Navigator, jsou tyto změny platné pro celý systém, ne pouze pro určitého uživatele nebo PC.

Použití trasování serveru VPN

Chcete-li prohlížet trasování serveru VPN, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)**, vyberte **Diagnostické nástroje** a potom **Trasování serveru**.

Chcete-li určit, jaký typ trasování má Správce klíčů VPN a Správce připojení VPN generovat, postupujte takto:

1. V okně **Trasování VPN** klepněte na ikonu

   (Volby).
2. Na straně **Správce připojení** určete typ trasování, který má spouštět server Správce připojení.
3. Na straně **Správce klíčů** určete typ trasování, který má spouštět server Správce klíčů.
4. Máte-li problémy s vyplněním strany nebo libovolného jejího pole, klepněte na **Nápověda**.
5. Klepnutím na tlačítko **OK** uložte provedené změny.
6. Klepnutím na ikonu

   (Spustit) trasování spustíte. Klepnutím na ikonu

   (Obnovit) můžete prohlížet nejnovější informace o trasování.

Prohlížení protokolů úloh serveru VPN

Chcete-li prohlížet aktuální protokoly úloh buď serveru Správce klíčů VPN, nebo serveru Správce připojení VPN, postupujte takto:

1. V prostředí produktu (TM) Navigator rozbalte svůj server **—> Síť —> Zásady pro práci s IP.**
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Diagnostické nástroje** a potom vyberte protokol úlohy serveru, který chcete prohlížet.

Prohlížení atributů Přidružení zabezpečení (SA)

Chcete-li prohlížet atributy Přidružení zabezpečení (SA), které jsou asociovány s aktivním připojením, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepněte pravým tlačítkem na příslušné aktivní připojení a vyberte **Přidružení zabezpečení**. V zobrazeném okně můžete prohlížet vlastnosti každého přidružení zabezpečení asociovaného s určitým připojením.

Ukončení připojení VPN

Chcete-li ukončit aktivní připojení na vyžádání, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepněte pravým tlačítkem na připojení, které chcete ukončit, a vyberte **Ukončit**. Chcete-li ukončit několik připojení, vyberte každé z nich jednotlivě, klepněte pravým tlačítkem a vyberte **Ukončit**.

Výmaz konfiguračních objektů VPN

Pokud opravdu chcete vymazat připojení VPN z databáze zásad VPN, postupujte takto:

1. V produktu iSeries(TM) Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepněte pravým tlačítkem na připojení, které chcete vymazat, a vyberte **Vymazat**.

Odstraňování problémů s VPN

VPN je komplexní rychle se rozvíjející technologie, která vyžaduje alespoň základní znalost standardních technologií IPSec. Musíte se také seznámit s pravidly IP paketů, protože VPN vyžaduje pro svou práci několik filtrovacích pravidel. Tato komplexnost může občas způsobit problémy s připojeními do VPN. Odstraňování problémů s VPN není vždy snadné. Musíte dobře znát systém a síťové prostředí a také komponenty, které používáte při správě systému a síťového prostředí. Níže uvedená témata obsahují pokyny, jak odstranit mnoho různých problémů, se kterými se můžete při používání VPN setkat:

- **Začínáme s odstraňováním problémů s VPN**
  Toto téma popisuje, jak lze vyhledat a opravit problémy s připojeními do VPN.
- **Běžné chyby konfigurace VPN a jejich řešení**
  Toto téma uvádí nejběžnější chyby a poskytuje možná řešení.
- **Odstraňování problémů s VPN pomocí žurnálu QIPFILTER**
  Toto téma uvádí informace o filtrovacích pravidlech VPN.
- **Odstraňování problémů s VPN pomocí žurnálu QVPN**
  Toto téma uvádí informace o IP provozu a připojeních.
- **Odstraňování problémů s VPN pomocí protokolů úloh VPN**
  Toto téma popisuje mnoho různých protokolů úloh, které VPN používá.
- **Odstraňování problémů s VPN trasováním komunikace operačního systému OS/400(R)**
  Toto téma popisuje, jak lze sledovat data na komunikační lince.

Začínáme s odstraňováním problémů s VPN

Existuje několik způsobů, jak začít analyzovat problémy s VPN:

1. Ujistěte se vždy, že jste použili nejnovější opravy PTF.
2. Zajistěte splnění minimálních požadavků na nastavení VPN.
3. Prostudujte všechny chybové zprávy nalezené v okně Informace o chybě nebo Protokoly úloh na serveru VPN v lokálním i vzdáleném systému. Při odstraňování problémů s připojením do VPN musíte často prohlédnout oba konce připojení. Musíte vzít také v úvahu, že musíte zkontrolovat čtyři adresy: lokální a vzdálené koncové systémy, což jsou adresy, ve kterých je použito IPSec na IP pakety, a lokální a vzdálené datové koncové systémy, které jsou zdrojovou a cílovou adresou IP paketů.
4. Pokud nalezené chybové zprávy neposkytují informace dostatečné k vyřešení problému, zkontrolujte žurnál IP filtr.
5. Trasování komunikace na serveru iSeries(TM) nabízí další místo, na kterém lze najít obecné informace o tom, zda lokální systém přijímá nebo odesílá požadavky na připojení.
6. Příkaz TRCTCPAPP (Trace TCP Application) poskytuje ještě další způsob, jak problém vyřešit. Servisní systém IBM (R) obvykle používá příkaz TRCTCPAPP a získává tak výstup o trasování, který mu pomůže analyzovat problémy s připojením.

Další kontrola

Pokud k chybě dojde po nastavení připojení a nejste si jisti, kde v síti se to stalo, pokuste se zredukovat složitost síťového prostředí. Místo zkoumání všech částí připojení VPN začněte například se samotným připojením do VPN. Následující seznam vám poskytuje několik základních rad, jak zahájit analýzu problémů s VPN, od nejjednoduššího až po složitější připojení VPN:

1. Začněte s konfigurací IP mezi lokálním a vzdáleným hostitelským systémem. Odstraňte filtr IP v rozhraní, které lokální i vzdálený systém používají pro komunikaci. Můžete testovat spojení z lokálního na vzdáleného hostitelského systému?

   Poznámka: Nezapomeňte v příkazu Testovat spojení zadat adresu vzdáleného systému a pomocí klávesy PF10 získat další parametry. Potom zadejte lokální IP adresu. Je to důležité zejména tehdy, když máte několik fyzických a logických rozhraní. Zajistíte tak umístění správných adres do paketů PING.

   Odpovíte-li **ano**, pokračujte krokem 2. Odpovíte-li **ne**, pak zkontrolujte svou IP konfiguraci, stav rozhraní a směrovací záznamy. Je-li konfigurace správná, zkontrolujte pomocí trasování komunikace, že například požadavek na testování spojení (PING) opustil systém. Odešlete-li požadavek na testování spojení (PING), ale neobdržíte-li odpověď, je problém pravděpodobně v síti nebo ve vzdáleném systému.

   Poznámka: Pomocné směrovače nebo ochranné bariéry (firewall) mohou provádět filtrování IP paketů a možná i filtrování paketů PING. Testování spojení pomocí příkazu PING je obvykle založeno na protokolu ICMP. Je-li testování spojení pomocí příkazu PING úspěšné, víte, že jste dosáhli připojitelnosti. Není-li testování spojení úspěšné, víte jen, že testování spojení pomocí příkazu PING selhalo. Připojitelnost můžete ověřit pomocí dalších IP protokolů, jako je například Telnet nebo FTP.
2. Zkontrolujte filtrovací pravidla pro VPN a zajistěte, aby byla aktivována. Spouští se filtrování úspěšně? Odpovíte-li **ano**, pokračujte krokem 3. Odpovíte-li **ne**, pak zkontrolujte chybové zprávy v okně Pravidla paketů v prostředí produktu iSeries Navigator. Zajistěte, aby ve filtrovacích pravidlech nebyl pro žádný provoz VPN zadán převod síťových adres (NAT).
3. Spuštění připojení VPN. Spouští se připojení úspěšně? Odpovíte-li **ano**, pokračujte krokem 4. Odpovíte-li **ne**, pak zkontrolujte chyby v protokolech úloh QTOVMAN a QTOKVPNIKE.
   Používáte-li VPN, musí váš poskytovatel služeb sítě Internet (ISP) a každá bezpečnostní komunikační brána podporovat protokoly AH (Authentication Header) a ESP (Encapsulated Security Payload). Výběr protokolu AH nebo ESP závisí na návrzích, které definujete pro připojení VPN.
4. Můžete aktivovat relaci uživatele přes připojení VPN? Odpovíte-li **ano**, pak připojení VPN funguje správně. Odpovíte-li **ne**, pak zkontrolujte pravidla paketů a skupiny a připojení VPN s dynamicky přiřazeným klíčem pro definice filtrů, které nepovolují požadovaný provoz uživatelů.

Běžné chyby konfigurace VPN a jejich řešení

Tato část popisuje některé z běžných problémů, se kterými se můžete v síti VPN setkat, a odkazuje vás na rady, které vám pomohou je vyřešit.

Poznámka: Při konfigurování VPN ve skutečnosti vytváříte různé konfigurační objekty, které jsou všechny nutné ke spuštění připojení. V termínech grafického uživatelského rozhraní VPN jsou těmito objekty Zásady zabezpečení IP a Zabezpečená připojení. Odkazují-li tyto informace na nějaký objekt, týkají se jedné nebo několika těchto částí VPN.

Chybové zprávy, které se běžně vyskytují

Zpráva	**Příznak**
TCP5B28	Při pokusu o aktivaci filtrovacích pravidel v rozhraní vyvoláte zprávu TCP5B28 o narušení pořadí CONNECTION_DEFINITION
Položka nebyla nalezena.	Klepnutím pravým tlačítkem na objekt VPN a buď výběrem **Vlastnosti**, nebo výběrem **Vymazat** vyvoláte zprávu **Položka nebyla nalezena**.
NEPLATNÝ PARAMETR PINBUF	Při pokusu o spuštění připojení vyvoláte zprávu **NEPLATNÝ PARAMETR PINBUF...**
Položka nebyla nalezena, vzdálený klíčový server...	Vyberete-li **Vlastnosti** u připojení s dynamicky přiřazeným klíčem, vyvoláte chybu, která říká, že server nemohl najít zadaný vzdálený klíčový server.

Nelze aktualizovat objekt	Klepnutím na tlačítko **OK** na listu vlastností pro skupinu s dynamicky přiřazeným klíčem nebo pro manuální připojení vyvoláte zprávu, která říká, že systém nemůže objekt aktualizovat.
Nelze zakódovat klíč...	Dostanete zprávu, která říká, že systém nemůže zakódovat vaše klíče, protože QRETSVRSEC musí mít hodnotu 1.
CPF9821	Při pokusu o rozbalení nebo otevření zásobníku zásad pro práci s IP v produktu iSeries(TM) Navigator se zobrazí zpráva CPF9821- Nemáte oprávnění k programu QTFRPRS v knihovně QSYS.

Další možné problémy

Chyba	**Příznak**
Všechny klíče jsou prázdné	Všechny předem nasdílené klíče pro připojení jsou při prohlížení vlastností manuálního připojení prázdné.
Objeví se přihlášení do jiného systému	Při prvním použití rozhraní pravidel paketů v prostředí produktu iSeries Navigator se zobrazí přihlášení do jiného než aktuálního systému.
Žádný stav připojení	Ve sloupci **Stav** v okně produktu iSeries Navigator chybí hodnota pro toto připojení.
Ukončená připojení jsou stále aktivní	Po ukončení připojení indikuje okno produktu iSeries Navigator, že připojení je stále aktivní.
3DES není pro šifrování k dispozici	Při práci s transformem zásady IKE, transformem zásady pro práci s daty nebo s manuálním připojením není šifrovací algoritmus 3DES k dispozici.
Neočekávané zobrazení sloupců	Nastavili jste sloupce, které chcete pro připojení VPN zobrazit v okně produktu iSeries Navigator. Když se na ně podíváte později, jsou zobrazeny jiné sloupce.
Aktivní filtrovací pravidla nelze deaktivovat	Při pokusu o deaktivaci aktuální množiny filtrovacích pravidel se v okně s výsledky zobrazí zpráva Selhala deaktivace aktivních pravidel.
Změna skupiny s dynamicky přiřazeným klíčem pro připojení	Při vytváření připojení s dynamicky přiřazeným klíčem zadáte skupinu s dynamicky přiřazeným klíčem a identifikátor pro vzdálený klíčový server. Když později prohlížíte vlastnosti souvisejícího připojeného objektu, zobrazuje stránka Obecné listu vlastností stejný identifikátor vzdáleného klíčového serveru, ale odlišnou skupinu s dynamicky přiřazeným klíčem.

Chybová zpráva VPN: TCP5B28

Příznak:

Při pokusu o aktivaci filtrovacích pravidel v rozhraní vyvoláte zprávu:

TCP5B28: Narušení pořadí CONNECTION_DEFINITION

Možné řešení:

Filtrovací pravidla, která se pokoušíte aktivovat, obsahovala definice připojení v jiném pořadí než v sadě pravidel aktivovaných v předchozím případě. Nejjednodušší způsob, jak chybu vyřešit, je aktivovat soubor s pravidly ve **všech rozhraních**, ne pouze v určitém rozhraní.

Chybová zpráva VPN: Položka nebyla nalezena

Příznak:

Když klepnete pravým tlačítkem na objekt v okně VPN (Virtual Private Networking) a vyberete buď **Vlastnosti** nebo **Vymazat**, objeví se následující zpráva:

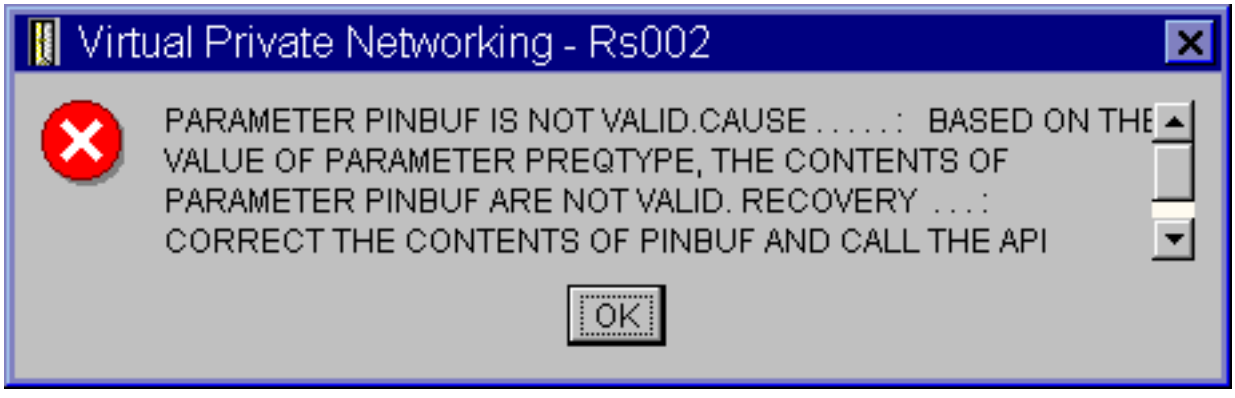
Možné řešení:

- Možná byl objekt vymazán nebo přejmenován a okno VPN (Virtual Private Networking) ještě nebylo obnoveno. V důsledku toho je objekt v okně ještě zobrazen. Chcete-li toto tvrzení ověřit, vyberte v menu **Zobrazení** příkaz **Obnovit**. Je-li objekt stále v okně VPN (Virtual Private Networking) zobrazen, pokračujte další položkou na tomto seznamu.
- Při konfiguraci vlastností objektu mohlo dojít k chybě v komunikaci mezi serverem VPN a serverem iSeries(TM). Mnohé objekty, které jsou zobrazeny v okně VPN (Virtual Private Networking) se vztahují k několika objektům v databázi zásad VPN. To znamená, že chyby v komunikaci mohou způsobit, že některé objekty v databázi se nadále vztahují k objektu ve VPN. Kdykoli vytvoříte nebo obnovíte objekt, dojde k chybě, když ve skutečnosti dojde ke ztrátě synchronizace. Jediný způsob, jak tento problém vyřešit je klepnout na tlačítko **OK** v okně chyby. Tím se pro objekt s chybou vyvolá list vlastností. V listu vlastností je vyplněno pouze pole jména. Všechna ostatní pole jsou prázdná (nebo obsahují předvolené hodnoty). Zadejte správné atributy objektu, klepněte na tlačítko **OK** a uložte změny.
- K podobné chybě dochází, když se pokoušíte objekt vymazat. Chcete-li tento problém vyřešit, vyplňte prázdný list vlastností, který se otevřel klepnutím na tlačítko **OK** v chybové zprávě. Tím aktualizujete všechny odkazy do databáze zásad VPN, které byly ztraceny. Potom můžete objekt vymazat.

Chybová zpráva VPN: NEPLATNÝ PARAMETR PINBUF

Příznak:

Při pokusu o spuštění připojení vyvoláte zprávu podobnou této:



Možné řešení:
Stává se to v případě, kdy je počítač nastaven na používání určitých lokalit, na které se malá písmena nemapují správně. Chcete-li tuto chybu opravit, zajistěte, aby všechny objekty používaly pouze velká písmena, nebo změňte lokalitu systému.

Chybová zpráva VPN: Položka nebyla nalezena, vzdálený klíčový server...

Příznak:
Vyberete-li **Vlastnosti** u připojení s dynamicky přiřazeným klíčem, vyvoláte chybu, která vypadá podobně jako tato:

Možné řešení:
Dochází k tomu, když vytvoříte připojení s identifikátorem určitého vzdáleného klíčového serveru a potom je tento vzdálený klíčový server ze skupiny s dynamicky přiřazeným klíčem odebrán. Chcete-li chybu vyřešit, klepněte na tlačítko **OK** na chybové zprávě. Otevře se list vlastností pro chybné připojení s dynamicky přiřazeným klíčem. Zde můžete buď přidat vzdálený klíčový server do skupiny s dynamicky přiřazeným klíčem, nebo vybrat identifikátor jiného vzdáleného klíčového serveru. Klepnutím na tlačítko **OK** na listu vlastností uložte provedené změny.

Chybová zpráva VPN: Nelze aktualizovat objekt

Příznak:
Klepnutím na tlačítko **OK** na listu vlastností pro skupinu s dynamicky přiřazeným klíčem nebo pro manuální připojení vyvoláte následující zprávu:

Možné řešení:
K této chybě dochází, když aktivní připojení používá objekt, který se pokoušíte změnit. Nelze provádět změny objektů v aktivním připojení. Chcete-li objekt změnit, určete nejprve příslušné aktivní připojení a potom klepněte pravým tlačítkem na **Ukončit** v zobrazeném kontextovém menu.

Chybová zpráva VPN: Nelze zakódovat klíč...

Příznak:
Zobrazí se tato chybová zpráva:

Možné řešení:
QRETSVRSEC je systémová hodnota, která ukazuje, zda systém může ukládat zakódované klíče. Je-li tato hodnota nastavena na 0, pak předem nasdílené klíče a klíče pro algoritmus v manuálním připojení nelze uložit do databáze zásad VPN. Chcete-li tento problém vyřešit, použijte relaci emulace 5250. Do příkazové řádky napište wrksysval a stiskněte klávesu **Enter**. V seznamu vyhledejte hodnotu QRETSVRSEC a vedle ní napište 2 (změna). V dalším podokně napište 1 a stiskněte klávesu **Enter**.

Chybová zpráva VPN: CPF9821

Příznak:
Když se v produktu iSeries(TM) Navigator pokoušíte rozbalit zásobník zásad pro práci s IP, objeví se zpráva CPF9821- Nemáte oprávnění k programu QTFRPRS v knihovně QSYS.

Možné řešení:
Možná nemáte požadované oprávnění k načtení aktuálního stavu pravidel paketů nebo k serveru Správce připojení VPN. Chcete-li mít přístup k funkcím pravidel paketů v produktu iSeries Navigator, musíte mít oprávnění *IOSYSCFG.

Chyba VPN: Všechny klíče jsou prázdné

Příznak:
Všechny předem nasdílené klíče a klíče algoritmů pro manuální připojení jsou prázdné.

Možné řešení:
K tomu dochází vždy, když systémová hodnota QRETSVRSEC je nastavena na hodnotu 0. Nastavení této systémové hodnoty na nulu smaže všechny klíče v databázi zásad VPN. Chcete-li problém vyřešit, nastavte tuto systémovou hodnotu na hodnotu 1 a zadejte znovu všechny klíče. Další informace najdete v části Chybová zpráva: Nelze šifrovat klíče.

Chyba VPN: Při použití pravidel paketů se objeví přihlášení k jinému systému

Příznak:
Při prvním použití pravidel paketů se objeví přihlášení k jinému systém, než je aktuální systém.

Možné řešení:
Pravidla paketů používají při ukládání pravidel zabezpečení do integrovaného systému souborů kódování Unicode. Dodatečné přihlášení umožňuje produktu iSeries(TM) Access získat příslušné převodní tabulky pro kódování Unicode. Tato situace nastane pouze jednou.

Chyba VPN: Prázdný stav připojení v okně iSeries Navigator

Příznak:
U připojení v okně produktu iSeries(TM) Navigator není žádná hodnota ve sloupci **Stav**.

Možné řešení:
Prázdná hodnota stavu značí, že připojení se právě spouští. To znamená, že ještě není spuštěno, ale zatím nedošlo k chybě. Když okno obnovíte, zobrazí se pro toto připojení jeden z těchto stavů: Chyba, Aktivní, Na žádost a Nečinný.

Chyba VPN: Připojení má aktivní stav i po ukončení

Příznak:
Okno produktu iSeries(TM) Navigator indikuje, že připojení je stále aktivní, i když jste ho již ukončili.

Možné řešení:
To se obvykle stává proto, že jste ještě neaktualizovali okno produktu iSeries Navigator. Okno tedy obsahuje zastaralé informace. Stačí vybrat v menu **Zobrazení** příkaz **Obnovit**.

Chyba VPN: 3DES není pro šifrování k dispozici

Příznak:
Při práci s transformem zásady IKE, transformem zásady pro práci s daty nebo s manuálním připojením není šifrovací algoritmus 3DES k dispozici.

Možné řešení:
Nejpravděpodobnější je, že máte v systému instalovaný produkt Cryptographic Access Provider AC2 (5722-AC2), ale potřebujete produkt Cryptographic Access Provider AC3 (5722-AC3). Produkt AC2 umožňuje pouze šifrovací algoritmus DES (Data Encryption Standard) kvůli omezením na délky klíčů.

Chyba VPN: V okně produktu iSeries Navigator se zobrazily neočekávané sloupce

Příznak:
Nastavili jste sloupce, které chcete pro připojení VPN zobrazit v okně produktu iSeries Navigator. Když se na ně podíváte později, jsou zobrazeny jiné sloupce.

Možné řešení:
Uvědomte si, že když změníte zobrazení sloupců v okně iSeries Navigator, jsou tyto změny platné pro celý systém, ne pouze pro určitého uživatele nebo PC. Když tedy někdo jiný změní sloupce v tomto okně, tyto změny mají dopad na každého, kdo prohlíží připojení v tomto systému.

Chyba VPN: Aktivní filtrovací pravidla nelze deaktivovat

Příznak:
Při pokusu o deaktivaci aktuální množiny filtrovacích pravidel se v okně s výsledky zobrazí zpráva Selhala deaktivace aktivních pravidel.

Možné řešení:
Tato zpráva obvykle znamená, že existuje alespoň jedno aktivní připojení VPN. Každé připojení se stavem aktivní musíte ukončit. K tomu stačí klepnout pravým tlačítkem na každé z aktivních připojení a vybrat **Ukončit**. Pak můžete filtrovací pravidla deaktivovat.

Chyba VPN: Změna skupiny s přiřazeným klíčem pro připojení

Příznak:
Při vytváření připojení s dynamicky přiřazeným klíčem zadáte skupinu s dynamicky přiřazeným klíčem a identifikátor pro vzdálený klíčový server. Když později vyberete **Vlastnosti** pro související připojený objekt, zobrazuje strana **Obecné** listu vlastností stejný identifikátor vzdáleného klíčového serveru, ale odlišnou skupinu s dynamicky přiřazeným klíčem.

Možné řešení:
Identifikátor je jedinou informací uloženou v databázi zásad VPN, která odkazuje na vzdálený klíčový server připojení s dynamicky přiřazeným klíčem. Při vyhledávání zásady pro vzdálený klíčový server vyhledá VPN první skupinu s dynamicky přiřazeným klíčem, která obsahuje tento identifikátor vzdáleného klíčového serveru. Prohlížíte-li vlastnosti jednoho z těchto připojení, zjistíte, že používá stejnou skupinu s dynamicky přiřazeným klíčem, jaká byla nalezena pomocí VPN. Pokud nechcete asociovat skupinu s dynamicky přiřazeným klíčem se vzdáleným klíčovým serverem, můžete provést jednu z následujících akcí:

1. Odstraňte vzdálený klíčový server ze skupiny s dynamicky přiřazeným klíčem.
2. Rozbalte **Podle skupin** v levém podokně rozhraní VPN a vyberte požadovanou skupinu s dynamicky přiřazeným klíčem a táhněte ji na horní okraj tabulky v pravém podokně. VPN pak bude při hledání identifikátoru vzdáleného klíčového serveru zkoumat nejprve tuto skupinu s dynamicky přiřazeným klíčem.

Odstraňování problémů s VPN pomocí žurnálu QIPFILTER

Žurnál QIPFILTER je umístěn v knihovně QUSRSYS a obsahuje informace o sadách filtrovacích pravidel a také o tom, zda byl IP datagram povolen či odepřen. Protokolování je prováděno na základě volby žurnálování, kterou zadáte ve filtrovacích pravidlech.

Aktivace žurnálu Filtr IP paketů

Chcete-li aktivovat žurnál QIPFILTER, použijte editor Pravidel paketů v produktu iSeries(TM) Navigator. Funkci protokolování musíte aktivovat pro každé jednotlivé filtrovací pravidlo. Neexistuje funkce, která aktivuje protokolování pro všechny datagramy přicházející do systému nebo z něj odcházející.

Poznámka: Chcete-li aktivovat žurnál QIPFILTER, musí být deaktivovány filtry.

Následující postup ukazuje, jak lze aktivovat žurnálování pro určité filtrovací pravidlo:

1. V produktu iSeries Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketu** a vyberte **Konfigurace**. Zobrazí se rozhraní Pravidla paketů.
3. Otevřete stávající soubor filtrovacích pravidel.
4. Dvakrát klepněte na filtrovací pravidlo, které chcete žurnálovat.
5. Na straně **Obecné** vyberte hodnotu **FULL** v poli **Žurnálování** jako ve výše uvedeném dialogu. Tím je protokolování pro toto filtrovací pravidlo aktivováno.
6. Klepněte na tlačítko **OK**.
7. Uložte a aktivujte změněný soubor filtrovacích pravidel.

Pokud IP datagram vyhovuje definicím ve filtrovacím pravidle, vytvoří se záznam v žurnálu QIPFILTER.

Použití žurnálu QIPFILTER

Operační systém OS/400(R) automaticky vytvoří žurnál, když poprvé aktivujete filtr IP paketu. Chcete-li prohlížet podrobnosti specifické pro záznam v žurnálu, můžete záznamy žurnálu zobrazit na obrazovce nebo můžete použít výstupní soubor.

Zkopírováním záznamů žurnálu do výstupního souboru můžete tyto záznamy snadno prohlížet pomocí dotazovacích obslužných programů, jako jsou například Query/400 a SQL. Můžete také napsat vlastní programy HLL, které zpracovávají záznamy ve výstupních souborech.

Následuje příklad příkazu DSPJRN (Display Journal):

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

Chcete-li zkopírovat záznamy žurnálu QIPFILTER do výstupního souboru, postupujte takto:

1. Vytvořte kopii výstupního souboru QSYS/QATOFIPF dodávaného systémem do uživatelské knihovny pomocí příkazu CRTDUPOBJ (Create Duplicate Object). Následuje příklad příkazu CRTDUPOBJ:

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

2. Zkopírujte záznamy ze žurnálu QUSRSYS/QIPFILTER do výstupního souboru vytvořeného v předchozím kroku pomocí příkazu DSPJRN (Display Journal).

Kopírujete-li DSPJRN do výstupního souboru, který neexistuje, systém ho vytvoří za vás, ale tento soubor neobsahuje správné popisy polí.

Poznámka: Žurnál QIPFILTER obsahuje pouze záznamy PERMIT a DENY pro filtrovací pravidla, ve kterých je volba žurnálování nastavena na hodnotu FULL. Pokud jste například nastavili pouze filtrovací pravidla PERMIT, budou odepřeny IP datagramy, které nejsou explicitně povoleny. Pro tyto odepřené datagramy nebudou do žurnálu přidány žádné záznamy. Kvůli analýze problémů byste mohli přidat filtrovací pravidlo, které explicitně odepře veškerý

další provoz a provádí úplné (FULL) žurnálování. Potom budete v žurnálu mít záznamy DENY pro všechny IP datagramy, které jsou odepřeny. S ohledem na výkon se nedoporučuje aktivovat žurnálování pro všechna filtrovací pravidla. Po otestování sad filtrů zredukujte žurnálování na únosnou míru.

Tabulku, která popisuje výstupní soubor QIPFILTER, najdete v části Pole žurnálu QIPFILTER.

Pole žurnálu QIPFILTER

Následující tabulka popisuje pole ve výstupním souboru QIPFILTER:

Jméno pole	Délka pole	Numerické	Popis	Poznámka
TFENTL	5	A	Délka záznamu	
TFSEQN	10	A	Pořadové číslo	
TFCODE	1	N	Kód žurnálu	Vždy M
TFENTT	2	N	Typ záznamu	Vždy TF
TFTIME	26	N	Označení času SAA	
TFJOB	10	N	Jméno úlohy	
TFUSER	10	N	Uživatelský profil	
TFNBR	6	A	Číslo úlohy	
TFPGM	10	N	Jméno programu	
TFRES1	51	N	Vyhrazeno	
TFUSPF	10	N	Uživatel	
TFSYMN	8	N	Jméno systému	
TFRES2	20	N	Vyhrazeno	
TFRESA	50	N	Vyhrazeno	
TFLINE	10	N	Popis linky	*ALL, pokud TFREVT je U* , prázdné, pokud TFREVT je L*, Jméno linky, pokud TFREVT je L
TFREVT	2	N	Událost pravidla	L* nebo L, když jsou pravidla zavedena. U*, když pravidla nejsou zavedena, A pro akci filtru
TFPDIR	1	N	Směr IP paketu	O je odchozí, I je příchozí
TFRNUM	5	N	Číslo pravidla	Platí pro číslo pravidla v souboru aktivních pravidel
TFACT	6	N	Akce filtru provedena	PERMIT, DENY nebo IPSEC
TFPROT	4	N	Transportní protokol	1 je ICMP 6 je TCP 17 je UDP 50 je ESP 51 je AH
TFSRCA	15	N	Zdrojová IP adresa	
TFSRCP	5	N	Zdrojový port	Přebytečný bajt, pokud TFPROT= 1 (ICMP)
TFDSTA	15	N	Cílová IP adresa	

Jméno pole	Délka pole	Numerické	Popis	Poznámka
TFDSTP	5	N	Cílový port	Přebytečný bajt, pokud TFPROT= 1 (ICMP)
TFTEXT	76	N	Další text	Obsahuje popis, pokud TFREVT= L* nebo U*

Odstraňování problémů s VPN pomocí žurnálu QVPN

VPN používá zvláštní žurnál pro protokolování informací o IP provozu a připojeních. Jmenuje se žurnál QVPN a je uložený v knihovně QUSRSYS. Jeho kód je M a typ žurnálu je TS. Záznamy žurnálu budete málokdy používat denně. Mohly by být užitečné při odstraňování problémů a ověřování, zda systém, klíče a připojení jsou funkční. Záznamy žurnálu vám například pomohou zjistit, co se stalo vašim datovým paketům. Také vás průběžně informují o stavu aktuálního připojení VPN.

Aktivace žurnálu VPN

Chcete-li aktivovat žurnál VPN, použijte rozhraní VPN v produktu iSeries(TM) Navigator. Neexistuje funkce, která aktivuje protokolování pro všechna připojení VPN. Proto musíte aktivovat funkci protokolování pro každou jednotlivou skupinu s dynamicky přiřazeným klíčem nebo manuální připojení.

Následující postup ukazuje, jak lze aktivovat funkci žurnálování pro určitou skupinu s dynamicky přiřazeným klíčem nebo manuální připojení.

1. V produktu iSeries Navigator rozbalte svůj server **—> Síť—> Zásady pro práci s IP—> VPN (Virtual Private Networking)—> Zabezpečená připojení**.
2. Pro skupiny s dynamicky přiřazeným klíčem rozbalte **Podle skupin** a potom klepněte pravým tlačítkem na skupinu s dynamicky přiřazeným klíčem, pro kterou chcete aktivovat žurnálování, a vyberte **Vlastnosti**.
3. Pro manuální připojení rozbalte **Všechna připojení** a potom klepněte pravým tlačítkem na manuální připojení, pro které chcete aktivovat žurnálování.
4. Na straně **Obecné** vyberte požadovanou úroveň žurnálování. Můžete si vybrat ze čtyř možností. Patří mezi ně:
   Žádné
   Pro tuto skupinu připojení nebude prováděno žádné žurnálování.
   Vše
   Žurnálování bude prováděno pro všechny aktivity připojení, jako je například spuštění a ukončení připojení nebo obnovení klíčů a informace o IP provozu.
   Aktivita připojení
   Žurnálování bude prováděno pro takové aktivity připojení, jako je spuštění a ukončení připojení.
   IP provoz
   Žurnálování bude prováděno pro veškerý provoz VPN, který je asociovaný s tímto připojením. Při každém vyvolání filtrovacího pravidla se vytvoří záznam protokolu. Systém zaznamená informace o IP provozu do žurnálu QIPFILTER, který je umístěn v knihovně QUSRSYS.
5. Klepněte na tlačítko **OK**.
6. Spuštěním připojení aktivujte žurnálování.

Poznámka: Před ukončením žurnálování se přesvědčte, že připojení již není aktivní. Chcete-li změnit stav žurnálování pro skupinu připojení, přesvědčte se, že s touto skupinou nejsou asociována žádná aktivní připojení.

Použití žurnálu VPN

Chcete-li prohlížet podrobnosti specifické pro záznam v žurnálu VPN, můžete záznamy žurnálu zobrazit na obrazovce nebo můžete použít výstupní soubor.

Zkopírováním záznamů žurnálu do výstupního souboru můžete tyto záznamy snadno prohlížet pomocí dotazovacích obslužných programů, jako je například Query/400 a SQL. Můžete také napsat vlastní programy HLL, které zpracovávají záznamy ve výstupních souborech. Následuje příklad příkazu DSPJRN (Display Journal):

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

Chcete-li zkopírovat záznamy žurnálu VPN do výstupního souboru, postupujte takto:

1. Vytvořte kopii výstupního souboru QSYS/QATOVSOF dodávaného systémem do uživatelské knihovny pomocí příkazu CRTDUPOBJ (Create Duplicate Object). Následuje příklad příkazu CRTDUPOBJ:

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

2. Zkopírujte záznamy ze žurnálu QUSRSYS/QVPN do výstupního souboru vytvořeného v předchozím kroku pomocí příkazu DSPJRN (Display Journal). Při pokusu o kopírování DSPJRN do výstupního souboru, který neexistuje, bude tento soubor systémem vytvořen, ale nebude obsahovat správné popisy polí.

Tabulku, která popisuje výstupní soubor QVPN, najdete v části Pole žurnálu QVPN.

Pole žurnálu QVPN

Následující tabulka popisuje pole ve výstupním souboru QVPN:

Jméno pole	Délka pole	Numerické	Popis	Poznámka
TSENTL	5	A	Délka záznamu	
TSSEQN	10	A	Pořadové číslo	
TSCODE	1	N	Kód žurnálu	Vždy M
TSENTT	2	N	Typ záznamu	Vždy TS
TSTIME	26	N	Označení času záznamu SAA	
TSJOB	10	N	Jméno úlohy	
TSUSER	10	N	Uživatel úlohy	
TSNBR	6	A	Číslo úlohy	
TSPGM	10	N	Jméno programu	
TSRES1	51	N	Nepoužito	
TSUSPF	10	N	Jméno uživatelského profilu	
TSSYNM	8	N	Jméno systému	
TSRES2	20	N	Nepoužito	
TSRESA	50	N	Nepoužito	
TSESDL	4	A	Délka specifických dat	
TSCMPN	10	N	Komponenta VPN	
TSCONM	40	N	Jméno připojení	
TSCOTY	10	N	Typ připojení	
TSCOS	10	N	Stav připojení	
TSCOSD	8	N	Počáteční datum	
TSCOST	6	N	Počáteční čas	
TSCOED	8	N	Koncové datum	
TSCOET	6	N	Koncový čas	
TSTRPR	10	N	Transportní protokol	
TSLCAD	43	N	Adresa lokálního klienta	
TSLCPR	11	N	Lokální porty	
TSRCAD	43	N	Adresa vzdáleného klienta	
TSCPR	11	N	Vzdálené porty	

Jméno pole	Délka pole	Numerické	Popis	Poznámka
TSLEP	43	N	Lokální koncový systém	
TSREP	43	N	Vzdálený koncový systém	
TSCORF	6	N	Časy obnovy	
TSRFDA	8	N	Datum příští obnovy	
TSRFTI	6	N	Čas příští obnovy	
TSRFLS	8	N	Velikost obnovy	
TSSAPH	1	N	Fáze SA	
TSAUTH	10	N	Typ autentizace	
TSENCR	10	N	Typ šifrování	
TSDHGR	2	N	Skupina Diffie-Hellman	
TSERRC	8	N	Chybový kód	

Odstraňování problémů s VPN pomocí protokolů úloh VPN

Když narazíte na problémy s připojeními do VPN, vždy je vhodné analyzovat protokoly úloh. Vlastně je několik protokolů úloh, které obsahují chybové zprávy a další informace, které souvisejí s prostředím VPN.

Je důležité provést analýzu protokolů úloh na obou stranách připojení, pokud jsou obě strany servery iSeries(TM). Když selže spuštění dynamického připojení, je užitečné vědět, co se děje ve vzdáleném systému.

V podsystému QSYSWRK jsou spuštěny tyto úlohy VPN: QTOVMAN a QTOKVPNIKE. V produktu OS/400(R) iSeries Navigator můžete prohlížet příslušné protokoly úloh.

Tato sekce uvádí nejdůležitější úlohy pro prostředí VPN. Následující seznam uvádí jména úloh a stručný popis jejich použití:

QTCPIP
Toto je základní úloha, která spouští všechna rozhraní TCP/IP. Máte-li obecně elementární problémy s protokolem TCP/IP, proveďte analýzu protokolu úlohy QTCPIP.

QTOKVPNIKE
Úloha QTOKVPNIKE je úloha serveru Správce klíčů VPN. Správce klíčů VPN naslouchá UDP portu 500 a provádí zpracování protokolu IKE (Internet Key Exchange).

QTOVMAN
Tato úloha spravuje připojení VPN. Související protokol úlohy obsahuje zprávy pro každý pokus o neúspěšné připojení.

QTPPANSxxx
Tato úloha se používá pro připojení PPP po komutované lince. Odpovídá na pokusy o připojení, ve kterých je parametr *ANS definován jako profil PPP.

QTPPPCTL
Toto je úloha PPP pro připojení odchozích hovorů po komutované lince.

QTPPPL2TP
Toto je úloha spravuje protokol L2TP (Layer Two Tunneling Protocol). Máte-li problémy při nastavení tunelu L2TP, vyhledejte zprávy v tomto protokolu úloh.

Běžné chybové zprávy serveru Správce připojení VPN

Tato část popisuje některé z běžnějších chybových zpráv serveru Správce připojení VPN, se kterými se můžete setkat.

Při výskytu chyby zaznamená Správce připojení VPN do protokolu úlohy obecně dvě zprávy. První zpráva poskytuje podrobnosti týkající se chyby. Informace o těchto chybách můžete v prostředí produktu iSeries(TM) Navigator zobrazit, když klepnete pravým tlačítkem na chybné připojení a vyberete **Informace o chybě**.

Druhá zpráva popisuje akci, kterou jste se pokoušeli s připojením provést, když došlo k chybě, například spuštění připojení nebo jeho ukončení. Níže popsané zprávy TCP8601, TCP8602 a TCP860A jsou typickými příklady těchto dvou zpráv.

Chybové zprávy serveru Správce připojení VPN

Zpráva	**Příčina**	**Obnova**
TCP8601 Připojení VPN [*jméno připojení*] nelze navázat.	Toto připojení VPN nelze navázat z důvodů popsaných jedním z těchto důvodových kódů: *0* - Předchozí zpráva v protokolu úlohy se stejným jménem připojení do VPN obsahuje podrobnější informace. *1* - Konfigurace zásad VPN. *2* - Selhání síťové komunikace. *3* - Došlo k selhání serveru Správce klíčů VPN při vyjednávání o novém přidružení zabezpečení. *4* - Vzdálený koncový systém tohoto připojení není správně konfigurován. *5* - Došlo k selhání serveru Správce klíčů VPN při odpovídání serveru Správce připojení VPN. *6* - Došlo k selhání při zavádění připojení IPSec do VPN. *7* - Došlo k selhání komponenty PPP.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Stav připojení můžete prohlížet pomocí produktu iSeries Navigator. Připojení, která nelze spustit, budou v chybovém stavu.
TCP8602 K chybě došlo ukončením připojení VPN [*jméno připojení*].	Bylo požadováno, aby zadané připojení VPN bylo ukončeno, ale nebylo ukončeno, nebo bylo ukončeno s chybou z důvodů popsaných jedním z těchto důvodových kódů: *0* - Předchozí zpráva v protokolu úlohy se stejným jménem připojení do VPN obsahuje podrobnější informace. *1* - Připojení VPN neexistuje. *2* - Selhání interní komunikace se serverem Správce klíčů VPN. *3* - Selhání interní komunikace s IPSec. *4* - Selhání komunikace se vzdáleným koncovým systémem připojení VPN.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Stav připojení můžete prohlížet pomocí produktu iSeries Navigator. Připojení, která nelze spustit, budou v chybovém stavu.

Zpráva	Příčina	Obnova
TCP8604 Spuštění připojení [*jméno připojení*] do VPN selhalo.	Spuštění připojení VPN selhalo z důvodů popsaných jedním z těchto důvodových kódů: *1* - Jméno vzdáleného hostitelského systému nelze převést na IP adresu. *2* - Jméno lokálního hostitelského systému nelze převést na IP adresu. *3* - Filtrovací pravidlo zásad VPN asociované s tímto připojením do VPN není zavedeno. *4* - Hodnota klíče zadaná uživatelem není platná pro asociovaný algoritmus. *5* - Počáteční hodnota pro připojení VPN nepovoluje zadanou akci. *6* - Systémová role pro připojení VPN není konzistentní s informacemi ze skupiny připojení. *7* - Vyhrazeno. *8* - Datové koncové systémy (lokální a vzdálené adresy a služby) tohoto připojení VPN nejsou konzistentní s informacemi ze skupiny připojení. *9* - Neplatný typ identifikátoru.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Zkontrolujte nebo opravte konfiguraci zásad VPN pomocí produktu iSeries Navigator. Zajistěte, aby skupina dynamických klíčů asociovaná s tímto připojením měla přijatelné konfigurované hodnoty.
TCP8605 Správce připojení VPN nemohl komunikovat se serverem Správce klíčů VPN.	Správce připojení VPN vyžaduje služby serveru Správce klíčů VPN, aby mohl vytvořit přidružení zabezpečení pro dynamická připojení VPN. Správce připojení VPN nemohl komunikovat se serverem Správce klíčů VPN.	1. Další zprávy najdete v protokolech úloh. 2. Pomocí příkazu NETSTAT OPTION(*IFC) ověřte, zda je rozhraní *LOOPBACK aktivní. 3. Ukončete server VPN příkazem ENDTCPSVR SERVER(*VPN). Potom server VPN restartujte příkazem STRTCPSRV SERVER(*VPN). **Poznámka:** Všechna aktuální připojení VPN tak budou ukončena.

Zpráva	Příčina	Obnova
TCP8606 Správce klíčů VPN nemohl vytvořit požadované přidružení zabezpečení pro připojení [*jméno připojení*].	Správce klíčů VPN nemohl vytvořit požadované přidružení zabezpečení z důvodů popsaných jedním z těchto důvodových kódů: *24* - Selhala autentizace připojení klíčů na serveru Správce klíčů VPN. *8300* - Došlo k selhání při vyjednávání připojení klíčů na serveru Správce klíčů VPN. *8306* - Nebyl nalezen lokální předem nasdílený klíč. *8307* - Nebyla nalezena žádná zásada vzdáleného připojení IKE fáze 1. *8308* - Nebyl nalezen vzdálený předem nasdílený klíč. *8327* - Vypršel časový limit pro vyjednávání připojení klíčů na serveru Správce klíčů VPN. *8400* - Došlo k selhání při vyjednávání připojení VPN na serveru Správce klíčů VPN. *8407* - Nebyla nalezena žádná vzdálená zásada IKE fáze 2. *8408* - Vypršel časový limit pro vyjednávání připojení VPN na serveru Správce klíčů VPN. *8500 nebo 8509* - Došlo k chybě sítě na serveru Správce klíčů VPN.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Zkontrolujte nebo opravte konfiguraci zásad VPN pomocí produktu iSeries Navigator. Zajistěte, aby skupina dynamických klíčů asociovaná s tímto připojením měla přijatelné konfigurované hodnoty.
TCP8608 Připojení VPN [*jméno připojení*] nemohlo získat adresu převodem síťových adres (NAT).	Tato skupina dynamických klíčů nebo připojení dat určuje, že převod síťových adres (NAT) bude proveden na jedné nebo více adresách a že došlo k selhání z důvodů popsaných jedním z těchto důvodových kódů: *1* - Adresa, na kterou má být převod síťových adres (NAT) aplikován, není jedinou IP adresou. *2* - Všechny dostupné adresy jsou již použity.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Zkontrolujte nebo opravte zásady VPN pomocí produktu iSeries Navigator. Zajistěte, aby skupina dynamických klíčů asociovaná s tímto připojením měla přijatelné hodnoty pro konfigurované adresy.
TCP8620 Lokální koncový systém připojení není k dispozici.	Toto připojení VPN nelze aktivovat, protože lokální koncový systém připojení není k dispozici.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Pomocí příkazu NETSTAT OPTION(*IFC) zkontrolujte, že lokální koncový systém připojení je definován a spuštěn. 3. Opravte všechny chyby a zopakujte požadavek.

Zpráva	Příčina	Obnova
TCP8621 Lokální datový koncový systém není k dispozici.	Toto připojení VPN nelze aktivovat, protože lokální datový koncový systém není k dispozici.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Pomocí příkazu NETSTAT OPTION(*IFC) zkontrolujte, že lokální koncový systém připojení je definován a spuštěn. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8622 Zapouzdření přenosu není s komunikační bránou povoleno.	Toto připojení VPN nelze aktivovat, protože zásada vyjednávání určila režim zapouzdření přenosu a toto připojení je definováno jako bezpečnostní komunikační brána.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Změňte zásadu VPN asociovanou s tímto připojením VPN pomocí produktu iSeries Navigator. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8623 Připojení VPN se překrývá se stávajícím připojením.	Toto připojení VPN nelze aktivovat, protože stávající připojení VPN je již aktivní. Toto připojení má lokální datový koncový systém [*hodnota lokálního datového koncového systému*] a vzdálený datový koncový systém [*hodnota vzdáleného datového koncového systému*].	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li prohlížet všechna aktivní připojení, která mají lokální a vzdálené datové koncové systémy, které se překrývají s tímto připojením, použijte produkt iSeries Navigator. Změňte zásadu stávajícího připojení, pokud jsou obě připojení vyžadována. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8624 Připojení VPN je mimo rozsah asociovaného filtrovacího pravidla zásad.	Toto připojení VPN nelze aktivovat, protože datové koncové systémy jsou mimo rozsah definovaného filtrovacího pravidla zásad.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zobrazit omezení datových koncových systémů pro toto připojení nebo skupinu dynamických klíčů, použijte produkt iSeries Navigator. Jsou-li vybrány volby **Podmnožina filtrů zásad** nebo **Přizpůsobení filtru zásad**, zkontrolujte datové koncové systémy tohoto připojení. Měly by vyhovovat aktivnímu filtrovacímu pravidlu, které má jméno akce IPSEC a jméno připojení VPN asociované s tímto připojením. Chcete-li toto připojení aktivovat, změňte zásadu stávajícího připojení nebo filtrovací pravidlo. 3. Opravte všechny chyby a zopakujte požadavek.

Zpráva	Příčina	Obnova
TCP8625 Selhala kontrola připojení VPN pomocí algoritmu protokolu ESP.	Toto připojení VPN nelze aktivovat, protože tajný klíč asociovaný s připojením je nedostatečný.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zobrazit zásadu asociovanou s tímto připojením a zadat jiný tajný klíč, použijte produkt iSeries Navigator. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8626 Koncový systém připojení VPN není stejný jako datový koncový systém.	Toto připojení VPN nelze aktivovat, protože zásada uvádí, že to je hostitelský systém a že koncový systém připojení VPN není stejný jako datový koncový systém.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zobrazit omezení datových koncových systémů pro toto připojení nebo skupinu dynamických klíčů, použijte produkt iSeries Navigator. Jsou-li vybrány volby **Podmnožina filtrů zásad** nebo **Přizpůsobení filtru zásad**, zkontrolujte datové koncové systémy tohoto připojení. Měly by vyhovovat aktivnímu filtrovacímu pravidlu, které má jméno akce IPSEC a jméno připojení VPN asociované s tímto připojením. Chcete-li toto připojení aktivovat, změňte zásadu stávajícího připojení nebo filtrovací pravidlo. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8628 Filtrovací pravidlo zásad není zavedeno.	Filtrovací pravidlo zásad není u tohoto připojení aktivní.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zobrazit aktivní filtry zásad, použijte produkt iSeries Navigator. Zkontrolujte filtrovací pravidlo zásad u tohoto připojení. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8629 Byl vypuštěn IP paket pro připojení VPN.	Toto připojení VPN má konfigurován převod síťových adres (NAT) a požadovaná sada adres překročila dostupné adresy NAT.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zvýšit počet adres NAT přiřazených tomuto připojení VPN, použijte produkt iSeries Navigator. 3. Opravte všechny chyby a zopakujte požadavek.
TCP862A Připojení profilu PPP se nezdařilo.	Toto připojení VPN bylo asociováno s profilem PPP. Po spuštění připojení byl proveden pokus o spuštění profilu PPP, ale došlo k chybě.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Zkontrolujte protokoly úlohy asociované s profilem PPP. 3. Opravte všechny chyby a zopakujte požadavek.

Odstraňování problémů s VPN pomocí trasování komunikace v systému OS/400

Systém OS/400(R) na serveru iSeries(TM) umožňuje trasování dat na komunikační lince, například rozhraní LAN nebo WAN. Průměrný uživatel možná nechápe celý obsah trasovacích dat. Z trasovacích položek však může určit, zda došlo k výměně dat mezi lokálním a vzdáleným systémem.

Začátek trasování komunikace
Trasování komunikace v systému zahájíte příkazem STRCMNTRC (Start Communications Trace). Následuje příklad příkazu STRCMNTRC:

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

Parametry příkazu jsou popsány v následujícím seznamu:

CFGOBJ (konfigurační objekt)
Jméno sledovaného konfiguračního objektu. Objekt je buď popis linky, popis síťového rozhraní, nebo popis síťového serveru.

CFGTYPE(typ konfigurace)
Zda se je sledována linka (*LIN), síťové rozhraní (*NWI), nebo síťový server (*NWS).

MAXSTG (velikost vyrovnávací paměti)
Velikost sledované vyrovnávací paměti. Předvolená hodnota je nastavena na 128 KB. Rozsah je od 128 KB až do 64 MB. Aktuální maximální velikost systémové vyrovnávací paměti v SST (System Service Tools). Použijete-li v příkazu STRCMNTRC vyrovnávací paměť o větší velikosti, než je uvedena v SST, můžete vyvolat chybovou zprávu. Uvědomte si, že součet velikostí vyrovnávacích pamětí zadaných ve všech trasováních komunikace nesmí překročit maximální velikost vyrovnávací paměti definovanou v SST.

DTADIR (směr dat)
Směr provozu, který má být sledován. Směrem může být pouze odchozí provoz (*SND), pouze příchozí provoz (*RCV), nebo oba (*BOTH).

TRCFULL (Plná paměť trasování)
Co se stane, když je vyrovnávací paměť pro trasování plná. Tento parametr může nabývat dvou hodnot. Předvolenou hodnotou je *WRAP. Znamená, že když je vyrovnávací paměť pro trasování plná, záznamy o trasování automaticky ″přetečou″ na začátek. Nejstarší záznamy o trasování budou přepsány novými tak, jak jsou zaznamenávány.

Druhá hodnota *STOPTRC ukončí trasování, když je vyrovnávací paměť pro trasování, jejíž velikost byla zadána parametrem MAXSTG, plná záznamů o trasování. Vyrovnávací paměť by měla být vždy zadávána tak, aby se do ní vešly všechny záznamy o trasování. Pokud trasování přetéká, můžete ztratit důležitá trasovací data. Pokud se tento problém často opakuje, definujte vyrovnávací paměť pro trasování tak velkou, aby přetékání nevyřadilo žádné důležité informace.

USRDTA (počet sledovaných bajtů uživatele)
Určuje velikost dat, která mají být sledována v části dat uživatele v datových rámcích. V rozhraní LAN je standardně sledováno pouze prvních 100 bajtů uživatelských dat. Ve všech ostatních rozhraních jsou sledována všechna uživatelská data. Pokud očekáváte problémy s uživatelskými daty rámce, přesvědčte se, že byla zadána hodnota *MAX.

TEXT (popis trasování)
Poskytuje smysluplný popis trasování.

Zastavení trasování komunikace
Pokud neurčíte jinak, trasování obvykle skončí, jakmile nastane podmínka, kterou sledujete. Trasování ukončíte příkazem ENDCMNTRC (End Communications Trace). Následující příkaz je příkladem příkazu ENDCMNTRC:

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

Tento příkaz má dva parametry:

CFGOBJ (konfigurační objekt)
Jméno konfiguračního objektu, pro který je trasování spuštěno. Objekt je buď popis linky, popis síťového rozhraní, nebo popis síťového serveru.

CFGTYPE (typ konfigurace)
Zda se je sledována linka (*LIN), síťové rozhraní (*NWI), nebo síťový server (*NWS).

Tisk trasovacích dat
Po ukončení trasování komunikace potřebujete trasovací data vytisknout. Použijte k tomu příkaz PRTCMNTRC (tisk trasování komunikace). Protože veškerý provoz na lince je v období trasování zaznamenáván, máte několik možností, jak generování výstupu filtrovat. Pokuste se ponechat soubory pro souběžný tisk co nejmenší. Urychlíte tak analýzu a zvýšíte její efektivitu. V případě problému s VPN filtrujte pouze IP provoz a určité IP adresy, pokud je to možné. Můžete také filtrovat určitý IP port. Následuje příklad příkazu PRTCMNTRC:

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

V tomto příkladu je trasování formátováno pro IP provoz a obsahuje pouze data pro IP adresy, jejichž zdrojovou nebo cílovou adresou je 10.50.21.1 a číslo zdrojového nebo cílového portu je 500.

Níže jsou vysvětleny pouze nejdůležitější parametry příkazů pro analýzu problémů s VPN:

CFGOBJ (konfigurační objekt)
Jméno konfiguračního objektu, pro který je trasování spuštěno. Objekt je buď popis linky, popis síťového rozhraní, nebo popis síťového serveru.

CFGTYPE (typ konfigurace)
Zda se je sledována linka (*LIN), síťové rozhraní (*NWI), nebo síťový server (*NWS).

FMTTCP (formátovat data TCP/IP)
Zda formátovat trasování pro data protokolu TCP/IP a UDP/IP. Zadejte *YES, chcete-li formátovat trasování pro IP data.

TCPIPADR (formátovat data TCP/IP podle adresy)
Tento parametr sestává ze dvou prvků. Zadáte-li v obou prvcích IP adresu, vytiskne se pouze IP provoz mezi těmito adresami.

SLTPORT (číslo IP portu)
Číslo IP portu pro filtrování.

FMTBCD (formátovat vysílání dat)
Zda tisknout všechny rámce vysílání. Předvolenou hodnotou je Yes. Pokud například nechcete požadavky protokolu ARP (Address Resolution Protocol), zadejte *NO. Jinak můžete být zaplaveni zprávami o vysílání.

Související informace pro VPN

Další scénáře a popisy konfigurace VPN najdete v těchto zdrojích informací:

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

Tato červená kniha IBM poskytuje podrobný popis procesu konfigurace tunelu VPN pomocí VPN verze V5R1 a integrované podpory protokolů L2TP a IPSec v operačním systému Windows 2000.

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

Tato červená kniha zkoumá koncepty VPN a popisuje implementaci VPN pomocí IPSec (IP security) a protokolu L2TP (Layer 2 Tunneling Protocol) v operačním systému OS/400.

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

Tato červená kniha zkoumá všechny integrované funkce zabezpečení, které jsou k dispozici v systému OS/400, například IP filtry, převod síťových adres (NAT), VPN, HTTP proxy server, SSL, DNS, přenos pošty, prověřování a protokolování. Popisuje jejich použití na praktických příkladech.

- **Virtual Private Networking: Securing Connections**

Tato webová stránka zdůrazňuje převratné novinky o VPN, uvádí nejnovější opravy PTF a odkazuje na další zajímavé webové stránky.

- **Další příručky a červené knihy týkající se zabezpečení**
  Přejděte sem a prohlédněte si seznam informací souvisejících se zabezpečením. Tento seznam je k dispozici online.

Chcete-li uložit PDF soubor na pracovní stanici, abyste ho později mohli prohlížet nebo tisknout, postupujte takto:

1. Klepněte pravým tlačítkem na PDF soubor v prohlížeči (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na **Uložit cíl jako...**.
3. Určete adresář, do kterého chcete PDF soubor uložit.
4. Klepněte na tlačítko **Uložit**.

Jestliže k prohlížení nebo tisku souborů ve formátu PDF potřebuje program Adobe Acrobat Reader, můžete si jeho kopii stáhnout z webové stránky Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabízet produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

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

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve vaší zemi, nebo písemně zastoupení IBM na adrese:

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

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, JAKÁ JE, BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který IBM považuje za odpovídající, bez vzniku jakýchkoli závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

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

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě IBM na programy nebo v jiné ekvivalentní smlouvě.

Všechny informace o provozu byly určeny v řízeném prostředí. Výsledky získané v jiném provozním prostředí se tudíž mohou výrazně lišit. Některá měření byla provedena v systémech s vývojovým prostředím a neexistuje žádná záruka, že tato měření budou stejná v obecně dostupných systémech. Kromě toho mohla být některá měření odhadnuta extrapolací. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit vhodnost dat pro svá specifická prostředí.

Informace, týkající se produktů jiných firem než IBM, byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy, které se týkají vlastností produktů jiných firem než IBM, musí být adresovány jejich dodavatelům.

Veškerá prohlášení, týkající budoucích trendů nebo strategií IBM, podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Všechny uvedené ceny jsou navrhované maloobchodní ceny IBM, jsou aktuální a podléhají změnám bez upozornění. Ceny prodejců se mohou lišit.

Tyto informace slouží pouze pro účely plánování. Informace zde uvedené podléhají změnám, dokud popsané produkty nebudou obecně dostupné.

Tyto publikace obsahují příklady údajů a sestav, používaných v každodenních obchodních činnostech. Abyste si udělali co neúplnější představu, obsahují příklady názvy konkrétních podniků, firemních značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami, používanými ve skutečných obchodních podnicích, je čistě náhodná.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro jsou ochranné známky společností International Business Machines Corporation a Lotus Development Corporation ve Spojených státech a případně v dalších jiných zemích.

C-bus je ochranná známka společnosti Corollary, Inc. ve Spojených státech a případně v dalších jiných zemích.

ActionMedia, LANDesk, MMX, Pentium a ProShare jsou ochranné známky nebo registrované ochranné známky společnosti Intel Corporation ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

SET a SET Logo jsou ochranné známky vlastněné společností SET Secure Electronic Transaction LLC.

Java a všechny ochranné známky založené na značce Java jsou ochranné známky společnosti Sun Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Názvy jiných společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných společností.

Ustanovení a podmínky pro stahování a tisk publikací

Oprávnění k používání publikací, které jste se rozhodli stáhnout, závisí na níže uvedených ustanoveních a podmínkách a na vašem potvrzení, že je akceptujete.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace a veškeré informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje její zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA. IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL.

Autorská práva na veškeré materiály náleží společnosti IBM Corporation.

Stažením nebo vytištěním publikace z tohoto serveru vyjadřujete svůj souhlas s těmito ustanoveními a podmínkami.

Vytištěno v Dánsku společností IBM Danmark A/S.