System i

Zabezpečení sítí VPN (Virtual private networking)

verze 6, vydání 1

System i

Zabezpečení sítí VPN (Virtual private networking)

verze 6, vydání 1

Poznámka

Přečtěte si informace v části “Poznámky”, na stránce 79 ještě před použitím těchto informací a produktu, který podporují.

Toto vydání se vztahuje na verzi 6, vydání 1, modifikaci 0 licencovaného programu IBM i5/OS (číslo produktu 5761-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 a zároveň poskytovat důležité funkce zabezpečení, jako je například autentizace a používání soukromých údajů.

VPN je volitelně instalovatelná komponenta produktu System i Navigator, který představuje grafické uživatelské rozhraní pro operační systém i5/OS. Umožňuje vám vytvořit zabezpečenou průběžnou cestu mezi libovolnou kombinací hostitelského systému a komunikační brány. 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 adresy IP 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 V6R1

Přečtěte si o informace o novinkách a významných změnách v kolekci témat týkajících se VPN.

Nová funkce: IP verze 6

Nyní můžete použít protokol IP verze 6 pro vytvoření VPN s následujícími typy připojení: hostitel na hostitele, hostitel na komunikační bránu a komunikační brána na komunikační bránu. Připojení VPN podporují protokol IP verze 6 v adrese, rozsahu, podsíti a jména hostitele. Všichni průvodci VPN byli aktualizováni pro přijetí nových typů ID protokolu IP verze 6.

- Protokol IP verze 6

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.

Soubor PDF pro VPN (Virtual private network)

Tento soubor ve formátu PDF můžete zobrazit a tisknout.

Chcete-li prohlížet nebo stáhnout tento dokument ve formátu PDF, klepněte na odkaz VPN (Virtual Private Networking) (přibližně 1100KB kB).

Jak ukládat soubory ve formátu PDF

Chcete-li uložit soubor PDF na pracovní stanici za účelem zobrazení nebo tisku:

1. Klepněte pravým tlačítkem myši na odkaz na PDF v prohlížeči.
2. Jestliže používáte aplikaci Internet Explorer, klepněte na **Uložit cíl jako**. Jestliže používáte aplikaci Netscape Communicator, klepněte na **Save Link As**.
3. Vyhledejte adresář, do něhož chcete soubor ve formátu PDF uložit.
4. Klepněte na **Uložit**.

Stažení produktu Adobe Acrobat Reader

Chcete-li tyto soubory PDF prohlížet nebo tisknout, potřebujete program Adobe Acrobat Reader. Bezplatnou kopii si můžete stáhnout z webových stránek společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Koncepce VPN

Je důležité mít alespoň základní znalost standardních technologií VPN, než budete implementovat 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 VPN používá:

Protokoly IP Security

Protokol IP Security (IPSec) poskytuje stabilní dlouhotrvající bázi pro poskytování síťového úrovňového zabezpečení.

IPSec 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 původu 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 ruční 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.

Poznámka: V závislosti na způsobu konfigurace IPSec mohou být některé konfigurace VPN zranitelné. Zranitelné mohou být konfigurace, ve kterých je IPSec nakonfigurován se zabezpečením ESP (Encapsulating Security Payload) v režimu důvěrného tunelu (s šifrováním), ale bez ochrany integrity (autentizace) nebo protokolu AH (Authentication Header). Předvolená konfigurace při vybrání ESP vždy zahrnuje autentizační algoritmus poskytující ochranu integrity. Proto pokud není autentizační algoritmus v transformu ESP odstraněn, jsou konfigurace VPN proti tomuto nebezpečí chráněny. Tato zranitelnost se netýká konfigurace VPN IBM Universal Connection.

Chcete-li zkontrolovat, zda se systému týká toto nebezpečí, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → Zásady zabezpečení IP → Zásady pro práci s daty**.
2. Klepněte pravým tlačítkem na metodu pro práci s daty, kterou chcete zkontrolovat a vyberte volbu **Vlastnosti**.
3. Klepněte na kartu **Návrhy**.
4. Vyberte jeden z návrhů ochrany dat, který používá protokol ESP a klepněte na volbu **Upravit**.
5. Klepněte na kartu **Transformy**.
6. Ze seznamu vyberte libovolné transformy, které používají protokol ESP a klepněte na volbu **Upravit**.
7. Zkontrolujte, zda Autentizační algoritmus má libovolnou jinou hodnotu než **Žádný**.

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

Tento seznam uvádí nejdůležitější protokoly IPSec:

Související pojmy

"Správa klíčů" na stránce 6
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.

Související informace

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. Zde je důležité zmínit se o tom, 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 dokument RFC naleznete na této 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 v některých oblastech zakázáno, zatímco použití protokolu AH není regulováno a může tedy být použit po celém světě.

Použití funkce ESN s protokolem AH

Při použití protokolu AH pravděpodobně budete chtít zapnout funkci ESN (Extended Sequence Number). Funkce ESN umožňuje přenos velkých objemů dat velkou rychlostí, aniž by bylo třeba znovu nastavovat klíč. Připojení VPN používá přes IPSec 64bitová pořadová čísla místo 32bitových. 64bitová čísla prodlužují čas před opětovným nastavením klíče, čímž se zamezí vyčerpání pořadových čísel a minimalizuje využití systémových prostředků.

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 dokumenty RFC naleznete na webové stránce: http://www.rfc-editor.org.

Související pojmy

“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.

Související informace

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. VPN používá při šifrování standardy DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 a AES (Advanced Encryption Standard).

Při použití algoritmu AES pro šifrování pravděpodobně budete chtít zapnout funkci ESN (Extended Sequence Number). Funkce ESN umožňuje přenos velkých objemů dat velkou rychlostí. Připojení VPN používá přes IPSec 64bitová pořadová čísla místo 32bitových. 64bitová čísla prodlužují čas před opětovným nastavením klíče, čímž se zamezí vyčerpání pořadových čísel a minimalizuje využití systémových prostředků.

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 dokumenty RFC naleznete na webové stránce: http://www.rfc-editor.org.

Protokol ESP používá při poskytování autentizačních funkcí algoritmy HMAC-MD5 a 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 formálně definuje protokol HMAC-MD5 v požadavku RFC Comments 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Společnost IETF formálně definuje protokol HMAC-SHA v požadavku RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Tyto a další dokumenty RFC naleznete na webové stránce: http://www.rfc-editor.org.

Související pojmy

"Protokol AH (Authentication Header)" na stránce 3
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.

Související informace

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

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.

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. 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. Některá řešení VPN vyžadují podpis RSA, aby systémy byly schopny spolupracovat. Například VPN v operačním systému Windows 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 připojení VPN pomocí produktu System i 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 dokumenty RFC naleznete na webové stránce: http://www.rfc-editor.org.

Související pojmy

“Scénář: Síť VPN vhodná pro bránu firewall” na stránce 28
V tomto scénáři chce velká pojišťovací společnost vytvořit síť VPN mezi bránou v Chicagu a hostitelským systémem v Minneapolis, přičemž obě sítě jsou za bránou firewall.

“Protokoly IP Security” na stránce 2
Protokol IP Security (IPSec) poskytuje stabilní dlouhotrvající bázi pro poskytování síťového úrovňového zabezpečení.

Související úlohy

“Konfigurace zásady IKE (Internet Key Exchange)” na stránce 46
Zásada IKE určuje, jakou úroveň autentizace a šifrování používá IKE při vyjednáváních fáze 1.

“Konfigurace zásad pro práci s daty” na stránce 47
Zásada pro práci s daty určuje, jaká úroveň autentizace nebo šifrování chrání data při postupu sítí VPN.

Související informace

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 společným síťovým systémům spravovat adresy IP 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 systém pobočky, která má být připojena ke společné síti pomocí systému komunikační brány s tunelem L2TP chráněným pomocí VPN.

Můžete si prohlédnout vizuální prezentaci o konceptu nepovinných tunelů L2TP chráněných pomocí IPSec. K tomu je potřeba modul plug-in 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).

Související pojmy

“Scénář: Ochrana nepovinného tunelu L2TP pomocí IPSec” na stránce 22
V tomto scénáři se dozvíte, jak nastavit připojení mezi hostitelským systémem pobočky a hlavní kanceláří společnosti, které používá tunel L2TP chráněný pomocí IPSec. Pobočka má dynamicky přiřazené adresy IP, zatímco společná kancelář má statické globálně směrovatelné adresy IP.

Převod síťových adres pro VPN

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.

Převod síťových adres (NAT) vezme soukromé adresy IP a převede je na veřejné adresy IP. 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 adresy IP mohou navíc kolidovat s podobnými příchozími adresami IP. 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 adresy IP 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 přidružena k připojení, 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 adres IP

Tento typ VPN NAT vám umožňuje vyvarovat se možných konfliktů adres IP, 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 adres IP, například 10.*.*.*. Způsob konfigurace tohoto typu VPN NAT závisí na tom, zda je systém iniciátorem připojení VPN nebo odpovídající stranou. Je-li systém iniciátorem připojení, převedete lokální adresy na adresy kompatibilní s adresami partnera připojení VPN. Je-li systém 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 adresy IP lokálního systému převodem jeho adres na jiné adresy, které budou veřejně dostupné. Při konfigurování VPN NAT můžete určit, aby každá veřejně známá adresa IP byla převedena na adresu z 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 systém 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 systémů, ke kterým mají mít lidé přístup pomocí VPN?
2. Potřebujete být flexibilní vzhledem ke skutečným adresám IP systému?
3. Máte jednu nebo několik globálně směrovatelných adres IP?

Scénář Použití převodu síťových adres pro VPN poskytuje příklad, jak konfigurovat VPN NAT tak, aby lokální adresy v modelu System i byly skryty.

Podrobné instrukce o nastavení VPN NAT v systému najdete v nápovědě online, která je k dispozici v rozhraní VPN v produktu System i Navigator.

Související pojmy

"Scénář: Použití převodu síťových adres pro VPN" na stránce 39
V tomto scénáři si chce vaše společnost vyměňovat citlivá data s jedním z obchodních partnerů pomocí připojení VPN. K další ochraně soukromých údajů své síťové struktury použije společnost také převod síťových adres VPN (VPN NAT), aby skryla soukromou adresu IP systému, který používá jako hostitelský systém aplikací, ke kterým má obchodní partner přístup.

"Pracovní formulář pro ruční připojení" na stránce 44
Vyplňte tento pracovní formulář ještě před konfigurováním ručního připojení.

IPSec kompatibilní s převodem síťových adres (NAT) s 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.

Problém: Konvenční převod síťových adres (NAT) přeruší VPN

Převod síťových adres (NAT) umožňuje skrýt neregistrované soukromé adresy IP za sadu registrovaných adres IP. To pomáhá chránit interní síť před vnějšími sítěmi. Převod síťových adres (NAT) také pomáhá zmírnit problém s vyčerpáním adres IP, 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. Kromě toho, ve verzi v5r2 může systém 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:

Po jeho zapouzdření odešle systém 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 pravidle filtrování. 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.

Související pojmy

“Scénář: Síť VPN vhodná pro bránu firewall” na stránce 28
V tomto scénáři chce velká pojišťovací společnost vytvořit síť VPN mezi bránou v Chicagu a hostitelským systémem v Minneapolis, přičemž obě sítě jsou za bránou firewall.

Protokol 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 dokument RFC naleznete na této webové stránce: http://www.rfc-editor.org.

Související informace

http://www.rfc-editor.org

VPN a IP filtrování

VPN a IP filtrování spolu úzce souvisejí. Většina připojení VPN vyžaduje pro řádné fungování pravidla filtrování. Toto téma uvádí, jaké filtry VPN vyžaduje, a seznamuje vás s koncepty filtrování souvisejícími s VPN.

Většina připojení VPN vyžaduje pro řádné fungování pravidla filtrování. Požadovaná pravidla filtrování 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. Síť může tato pravidla VPN generovat automaticky. Kdykoli je to možné, dovolte, ať VPN generuje filtry zásad za vás. Nejen že to pomůže eliminovat chyby, ale také nutnost konfigurovat pravidla jako samostatný krok pomocí editoru pravidel paketů v produktu System i 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:

Související pojmy

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Připojení VPN bez filtrů zásad

Pokud koncové systémy připojení VPN jsou samostatné specifické adresy IP a chcete spustit VPN, aniž byste v systému museli psát či aktivovat pravidla filtrování, můžete konfigurovat dynamický filtr zásad.

Pravidlo filtrování zásad určuje, které adresy, protokoly a porty mohou používat VPN a nasměruje příslušný provoz tímto připojením. V některých případech potřebujete konfigurovat připojení, které pravidlo filtrování 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 systém.
- Datové koncové systémy připojení musí být samostatné systémy. To znamená, že to nemohou být podsítě ani rozmezí adres.
- Pro připojení nesmí být zavedeno žádné pravidlo filtrování 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

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 pravidla filtrování napsaná explicitně pro povolení provozu IKE, pak systém implicitně provoz IKE povolí.

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 pravidla filtrování 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 pravidlech filtrování.

Scénáře: VPN

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

Související pojmy

Scénář QoS: Zabezpečené a předvídatelné výsledky (VPN a QoS)

Související informace

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

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

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

Scénář: Základní připojení pobočky

V tomto scénáři chce vaše společnost vytvořit VPN mezi podsítěmi svých vzdálených oddělení prostřednictvím dvojice modelů System i, které fungují jako komunikační brány VPN.

Situace

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 bran 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.

Důležité: Tento scénář ukazuje modelové bezpečnostní komunikační brány serveru System i připojené přímo k Internetu. Absence brány firewall má za úkol zjednodušit scénář. Neznamená to, že použití brány firewall není nutné. Ve skutečnosti musíte zvážit všechna bezpečnostní rizika spojená s každým připojením k Internetu.

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 systémům a prostředkům 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 adres IP v každé vzdálené podsíti eliminuje nutnost přidělit každému klientovi platnou veřejnou adresu IP.

Cíle

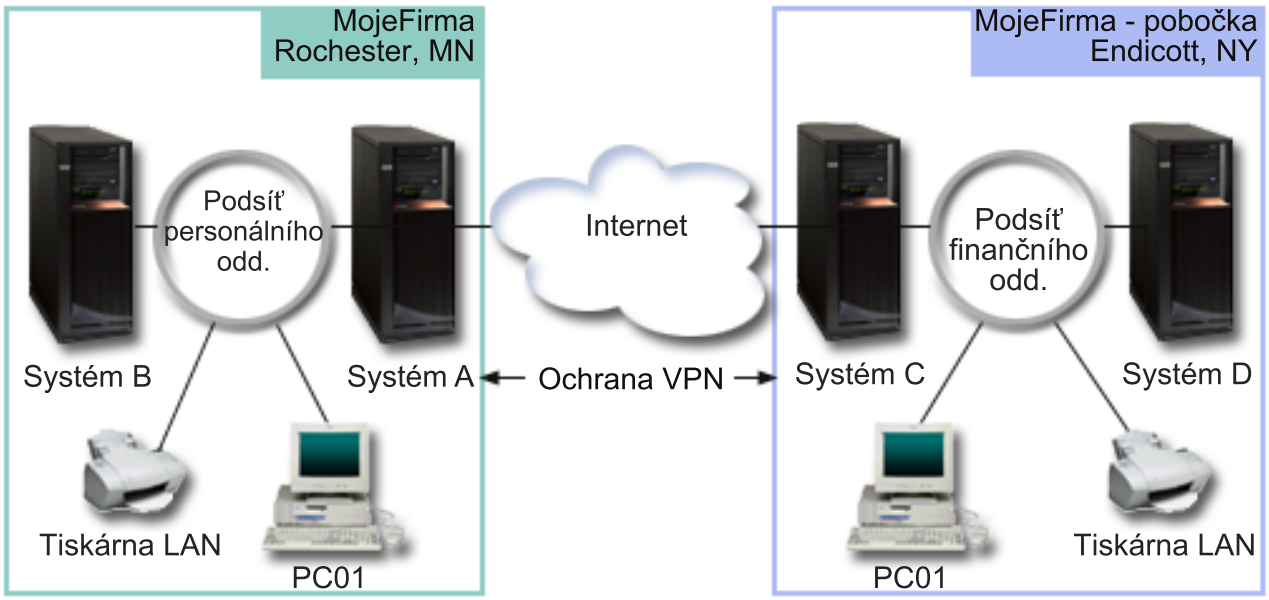
V tomto scénáři chce společnost MyCo, Inc. vytvořit VPN mezi podsítěmi svého personálního a finančního oddělení prostřednictvím páru modelů System i. Oba tyto systémy budou mít roli komunikačních bran VPN. V termínech konfigurace VPN provádí komunikační brána správu klíčů a používá IPSec na data, která 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 systém 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

- Systém A běží na operačním systému i5/OS verze 5, vydání 3 (V5R3) nebo novějším 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.
- Systém A je připojen k Internetu s adresou IP 204.146.18.227. Toto je koncový systém připojení. Systém A tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy.
- Systém A je ke svým podsítím připojen s adresou IP 10.6.11.1.
- Systém A je provozní systém v podsíti personálního oddělení, který provozuje standardní aplikace TCP/IP.

Finanční oddělení

- Systém C běží na operačním systému i5/OS verze 5, vydání 3 (V5R3) nebo novějším 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.
- Systém C je připojen k Internetu s adresou IP 208.222.150.250. Toto je koncový systém připojení. Systém C tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy.
- Systém C je ke svým podsítím připojen s adresou IP 10.196.8.5.

Úkoly konfigurace

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

Poznámka: Před zahájením těchto úloh ověřte směrování protokolu TCP/IP, aby bylo zajištěno, že oba systémy - komunikační brány 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.

Související pojmy

Směrování a vyvažování zatížení TCP/IP

Související informace

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

Vyplnění pracovních formulářů pro plánování

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 aplikujte na systém A. Tento postup zopakujte pro systém C s příslušnými adresami IP.

Tabulka 1. Systémové požadavky

Kontrolní seznam nezbytných předpokladů	**Odpovědi**
Běží na systému operační systém i5/OS V5R3 nebo novější?	Ano
Je nainstalována volba Digital Certificate Manager?	Ano
Je produkt System i Access for Windows nainstalovaný?	Ano
Je produkt System i Navigator nainstalovaný?	Ano
Je podkomponenta Síť produktu System i Navigator nainstalovaná?	Ano
Je produkt IBM TCP/IP Connectivity Utilities for i5/OS nainstalovaný?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano
Máte v systému 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 bránami firewall nebo směrovači, které používají filtrování IP paketů, podporují pravidla filtrování bran firewall a směrovačů protokoly AH a ESP?	Ano
Jsou brány firewall nebo směrovače konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	Ano
Jsou brány firewall konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Tabulka 2. Konfigurace VPN

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 vyžadujete v systému pro ochranu klíčů?	Vyvážený
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Nezadávejte hodnotu topsecretstuff.
Jaký je identifikátor lokálního klíčového serveru?	Adresa IP: 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?	Adresa IP: 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 vyžadujete v systému pro ochranu dat?	Vyvážený
Na která rozhraní budou připojení použita?	TRLINE

Konfigurace sítě VPN na systému A

Proveďte tuto úlohu pro konfiguraci systému A.

Použijte informace z pracovních formulářů a konfigurujte VPN na systému A:

1. V prostředí produktu System i Navigator rozbalte **Systém 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. Volitelně 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 **Adresa IP verze 4**.
15. V poli **Adresa IP** 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 podsítě** zadejte 255.255.0.0.
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 podsítě** 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**.
31. Vyberte **Použít k ochraně dat šifrovací algoritmus RC4**.
32. Klepnutím na tlačítko **Další** přejděte na stranu **Rozhraní aplikací**.
33. V tabulce **Linka** vyberte **TRLINE**.
34. Klepnutím na tlačítko **Další** přejděte na stranu **Souhrn**. Zkontrolujte, zda jsou průvodcem vytvořené objekty správné.
35. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci.
36. Když se zobrazí dialog **Aktivovat filtry zásad**, vyberte **Ano, aktivovat vytvořené filtry zásad** a potom vyberte **Povolit další přenosy**.
37. Klepnutím na tlačítko **OK** dokončete konfiguraci. Na výzvu uveďte, že chcete aktivovat pravidla ve všech rozhraních.

Související úlohy

"Konfigurace sítě VPN na systému C"
Postupujte stejně jako při konfiguraci VPN na systému A, ale podle potřeby změňte adresy IP. Jako vodítko použijte pracovní formuláře.

Konfigurace sítě VPN na systému C

Postupujte stejně jako při konfiguraci VPN na systému A, ale podle potřeby změňte adresy IP. Jako vodítko použijte pracovní formuláře.

Když dokončíte konfigurování komunikační brány VPN pro finanční oddělení, budou připojení ve stavu *na vyžádání*, 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.

Související úlohy

"Konfigurace sítě VPN na systému A" na stránce 15
Proveďte tuto úlohu pro konfiguraci systému A.

Spuštění VPN

Poté, co jste nakonfigurovali připojení VPN na systémech A a C, musíte připojení VPN spustit.

Chcete-li spustit VPN, proveďte následující kroky:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**.

Testování spojení

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

Chcete-li testovat připojení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém A → Síť**.
2. Klepněte pravým tlačítkem na **Konfigurace TCP/IP** a vyberte **Obslužné programy** a potom vyberte **Testovat spojení**.

3. V dialogovém okně **Testování spojení** v poli **Systém C** zadejte Testovat spojení.
4. Klepnutím na tlačítko **Testovat spojení ihned** ověřte připojitelnost ze systému A na systém B.
5. Když skončíte, klepněte na tlačítko **OK**.

Scénář: 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.

Situace

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

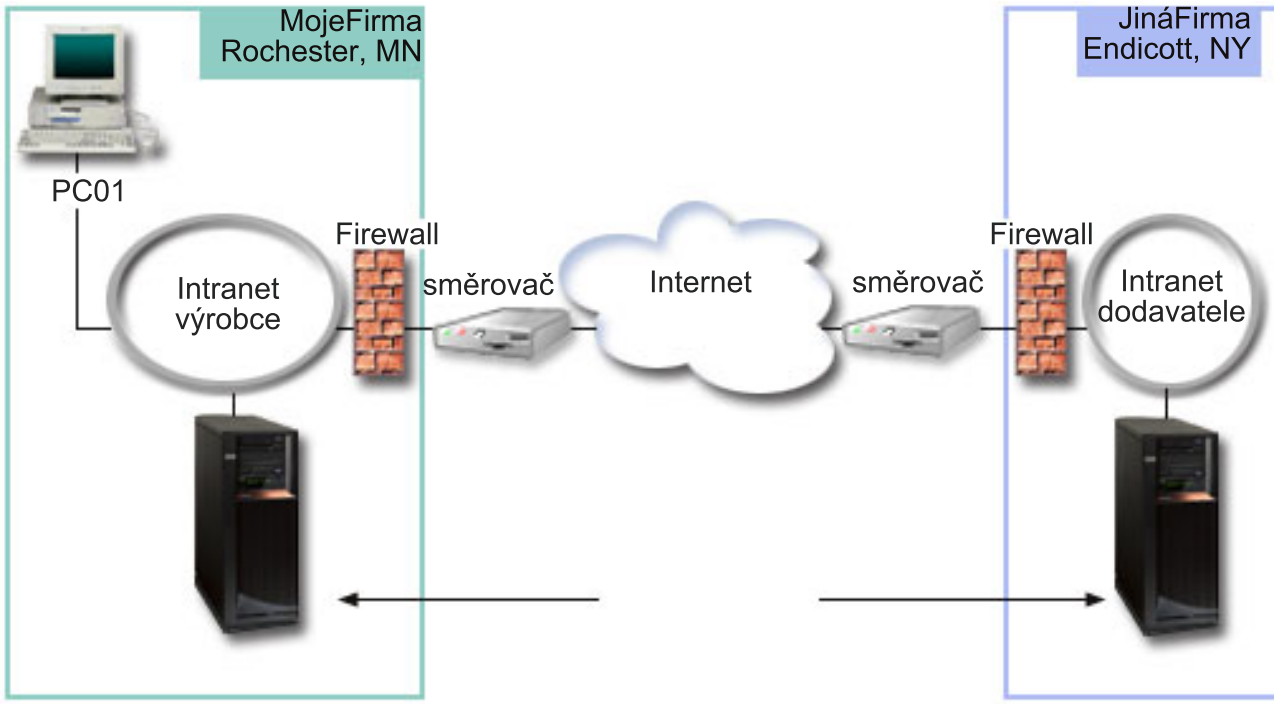
V tomto scénáři chce společnost MyCo vytvořit síť VPN mezi hostitelským systémem v sekci součástek a hostitelským systémem ve výrobním oddělení jednoho ze svých obchodních partnerů, firmy TheirCo.

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.

Důležité: 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 brány firewall, požadavky na adresy IP a směrování.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítí společností MyCo a TheirCo.



Dodavatelská síť společnosti MyCo

- Systém A běží na operačním systému i5/OS verze 5, vydání 3 (V5R3) nebo novějším.
- Systém A má adresu IP 10.6.1.1. Toto je koncový systém připojení a také datový koncový systém. Systém A navazuje připojení IKE a používá IPSec na příchozí a odeslané IP datagramy a je také zdrojem i cílem pro data, která procházejí VPN.
- Systém A je v podsíti 10.6.0.0 s maskou 255.255.0.0
- Pouze systém A může iniciovat připojení k systému C.

Výrobní síť společnosti TheirCo

- Systém C běží na operačním systému i5/OS verze 5, vydání 3 (V5R3) nebo novějším.
- Systém C má adresu IP 10.196.8.6. Toto je koncový systém připojení a také datový koncový systém. Systém A navazuje připojení IKE a používá IPSec na příchozí a odeslané IP datagramy a je také zdrojem i cílem pro data, která procházejí VPN.
- Systém 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:

Poznámka: Před zahájením těchto úloh ověřte směrování protokolu TCP/IP, aby bylo zajištěno, že oba systémy - komunikační brány 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.

Související pojmy

Směrování a vyvažování zatížení TCP/IP

Vyplnění pracovních formulářů pro plánování

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 aplikujte na systém A. Tento postup zopakujte pro systém C s příslušnými adresami IP.

Tabulka 3. Systémové požadavky

Kontrolní seznam nezbytných předpokladů	**Odpovědi**
Běží na systému operační systém i5/OS V5R3 nebo novější?	Ano
Je nainstalována volba Digital Certificate Manager?	Ano
Je produkt System i Access for Windows nainstalovaný?	Ano
Je produkt System i Navigator nainstalovaný?	Ano
Je podkomponenta Síť produktu System i Navigator nainstalovaná?	Ano
Je produkt IBM TCP/IP Connectivity Utilities for i5/OS nainstalovaný?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano
Máte v systému 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 bránami firewall nebo směrovači, které používají filtrování IP paketů, podporují pravidla filtrování bran firewall a směrovačů protokoly AH a ESP?	Ano
Jsou brány firewall nebo směrovače konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	Ano
Jsou brány firewall konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Tabulka 4. Konfigurace VPN

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 vyžadujete v systému pro ochranu klíčů?	Vyvážený
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Nezadávejte hodnotu topsecretstuff.
Jaký je identifikátor lokálního klíčového serveru?	Adresa IP: 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?	Adresa IP: 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 vyžadujete v systému pro ochranu dat?	Vyvážený
Na která rozhraní budou připojení použita?	TRLINE

Konfigurace sítě VPN na systému A

Chcete-li konfigurovat připojení k síti VPN na systému A, proveďte následující kroky.

Použijte informace z pracovních formulářů a konfigurujte VPN na systému A:

1. V prostředí produktu System i Navigator rozbalte **Systém → 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. Volitelně 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, který reprezentuje systém 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 **Adresa IP verze 4** . Přidružená adresa IP 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** vyberte 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 systém 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.

Konfigurace sítě VPN na systému C

Postupujte stejně jako při konfiguraci VPN na systému A, ale podle potřeby změňte adresy IP. Jako vodítko použijte pracovní formuláře.

Když dokončíte konfigurování komunikační brány VPN pro finanční oddělení, budou připojení ve stavu *na vyžádání*, 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.

Aktivace pravidel paketů

Průvodce VPN automaticky vytvoří pravidla paketů, která toto připojení požaduje, aby pracovalo správně. Musíte je ale aktivovat v obou systémech ještě před připojením do VPN.

Chcete-li aktivovat pravidla paketů na systému A, proveďte tyto kroky:

1. V prostředí produktu System i Navigator rozbalte **Systém 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. Opakujte tento postup, chcete-li aktivovat pravidla paketů na systému C.

Spuštění připojení

Poté, co jste nakonfigurovali připojení VPN, musíte připojení VPN spustit.

Chcete-li navázat připojení MyCo2TheirCo ze systému A:

1. V prostředí produktu System i Navigator rozbalte **Systém 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 → 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*.

Testování spojení

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

Chcete-li testovat připojení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém A → Síť**.
2. Klepněte pravým tlačítkem na **Konfigurace TCP/IP** a vyberte **Obslužné programy** a potom vyberte **Testovat spojení**.
3. V dialogovém okně **Testování spojení** v poli **Systém C** zadejte Testovat spojení.
4. Klepnutím na tlačítko **Testovat spojení ihned** ověřte připojitelnost ze systému A na systém B.
5. Když skončíte, klepněte na tlačítko **OK**.

Scénář: Ochrana nepovinného tunelu L2TP pomocí IPSec

V tomto scénáři se dozvíte, jak nastavit připojení mezi hostitelským systémem pobočky a hlavní kanceláří společnosti, které používá tunel L2TP chráněný pomocí IPSec. Pobočka má dynamicky přiřazené adresy IP, zatímco společná kancelář má statické globálně směrovatelné adresy IP.

Situace

Předpokládejme, že vaše společnost má malou pobočku v jiném státu. V průběhu libovolného pracovního dne může pobočka vyžadovat přístup k důvěrným informacím o modelu System i, 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).

Důležité: Tento scénář ukazuje bezpečnostní komunikační brány připojené přímo k Internetu. Absence brány firewall má za úkol zjednodušit scénář. Neznamená to, že použití brány firewall není nutné. Musíte uvážit všechna bezpečnostní rizika spojená s každým připojením k Internetu.

Cíle

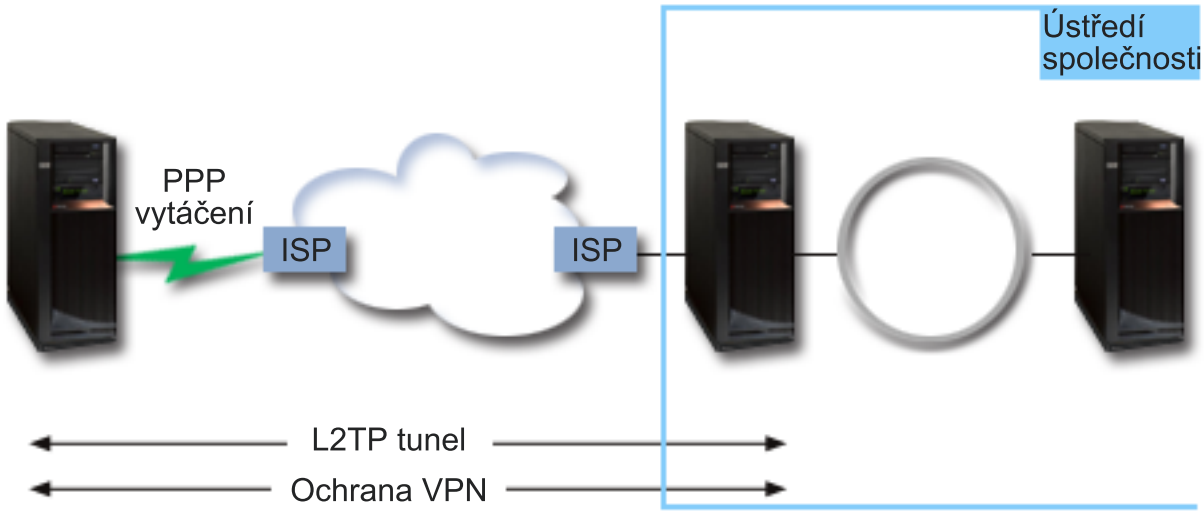
V tomto scénáři se systém pobočky připojí ke společné síti přes systém komunikační brány s tunelem L2TP chráněným VPN.

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:



Systém A

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

Systém B

- Musí mít přístup k aplikacím TCP/IP na systému 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 adresou IP 205.13.237.6. Toto je koncový systém připojení. Systém B tedy provádí správu klíčů a používá IPSec na příchozí a odeslané IP datagramy. Systém B je ke svým podsítím připojen s adresou IP 10.6.11.1.

Prostřednictvím L2TP jedná server *Systém A* jako iniciátor L2TP a server *Systém B* jedná jako ukončovač L2TP.

Úkoly konfigurace

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

Související pojmy

“Protokol L2TP (Layer 2 Tunnel Protocol)” na stránce 7
Připojení protokolu L2TP (Layer 2 Tunnel Protocol), které také nazýváme virtuální linky, poskytují nákladově efektivní přístup vzdáleným uživatelům tím, že umožňují společným síťovým systémům spravovat adresy IP přiřazené vzdáleným uživatelům. Připojení L2TP dále poskytují zabezpečený přístup k systémům a sítím, když je používáte ve spojení s IPSec (IP Security).

Související informace

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

Konfigurace sítě VPN na systému A

Chcete-li konfigurovat připojení k síti VPN na systému A, proveďte následující kroky.

Použijte informace z pracovních formulářů a konfigurujte VPN na systému A:

1. **Konfigurujte zásady IKE (Internet Key Exchange).**
   a. V prostředí produktu System i Navigator rozbalte Systém A → **Síť** → **Zásady pro práci s IP** → **VPN** → **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 **Adresa IP verze 4** a potom do pole **Adresa IP** 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 adresu IP, která není předem známa. Systém B používá tento identifikátor k identifikaci systému B, když systém B iniciuje připojení.
   g. Klepnutím na **Přidat** na straně **Transformy** přidejte transformy, které systém A navrhne systému 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. Klepnutím na tlačítko **OK** se vraťte na stranu **Transformy**.
   g. Zadejte hodnotu pro ukončení platnosti klíče.
   h. Klepnutím na tlačítko **OK** uložte nové zásady pro práci s daty.
3. **Konfigurace skupiny s dynamicky přiřazeným klíčem**
   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 **Metoda pro práci s daty** vyberte metodu pro práci s daty l2tpremoteuser, kterou jste vytvořili v kroku **Konfigurace metody pro práci s daty**.

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

h. Přejděte na stranu **Připojení**. Vyberte **Generovat následující pravidlo filtrování 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.

4. **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 systému 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 **Adresa IP** vyberte 205.13.237.6.

f. Zrušte označení **Spustit na vyžádání**.

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.

Související úlohy

“Konfigurace sítě VPN na systému B” na stránce 27
Chcete-li konfigurovat připojení VPN na systému B, postupujte stejně jako při konfiguraci připojení VPN na systému A a změňte podle potřeby adresy IP a identifikátory.

Konfigurace profilu připojení PPP a virtuální linky pro systém A

Nyní, když je na systému A nakonfigurováno připojení k síti VPN, musíte vytvořit profil PPP pro systém 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 systém A, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém 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 vyžádání (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. Volitelně můžete zadat 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 SystemA.
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 předchozím kroku “Konfigurace sítě VPN na systému A” na stránce 24.
17. Přejděte na stranu **Nastavení TCP/IP**.
18. V sekci **Adresa IP lokálního systému** vyberte **Přiřazená vzdáleným systémem**.
19. V sekci **Adresa IP vzdáleného systému** vyberte **Použít pevnou adresu IP**. Zadejte 10.6.11.1, což je adresa IP 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 systém 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 uživatele 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)**. V sekci Identifikace lokálního systému vyberte **Povolit vzdálenému systému ověřit identitu tohoto systému**.
28. Zadejte jméno uživatele SystemA a heslo.
29. Klepnutím na tlačítko **OK** uložte profil PPP.

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.

Chcete-li přidružit skupinu s dynamicky přiřazeným klíčem k profilu PPP, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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 "Konfigurace profilu připojení PPP a virtuální linky pro systém A" na stránce 25.
4. Klepnutím na tlačítko **OK** použijte l2tptocorp na profil PPP toCorp.

Konfigurace sítě VPN na systému B

Chcete-li konfigurovat připojení VPN na systému B, postupujte stejně jako při konfiguraci připojení VPN na systému A a změňte podle potřeby adresy IP a identifikátory.

Než začnete, vezměte v úvahu tyto skutečnosti:

- Označte vzdálený klíčový server identifikátorem klíče, který jste zadali pro lokální klíčový server na systému A. Například thisisthekeyid.
- Použijte *přesně* stejný předem nasdílený klíč.
- Přesvědčte se, že vaše transformy odpovídají transformům konfigurovaným na systému 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 vyžádání.

Související úlohy

"Konfigurace sítě VPN na systému A" na stránce 24
Chcete-li konfigurovat připojení k síti VPN na systému A, proveďte následující kroky.

Konfigurace profilu připojení PPP a virtuální linky pro systém B

Nyní, když je na systému B nakonfigurováno připojení k síti VPN, musíte vytvořit profil PPP pro systém B. 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 systém B, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém 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. Volitelně můžete zadat popis profilu.
9. Přejděte na stranu **Připojení**.
10. Vyberte adresu IP 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 SystemB.
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 **Adresa IP lokálního systému** vyberte pevnou adresu IP lokálního systému: 10.6.11.1.

18. V sekci **Adresa IP vzdáleného systému** vyberte jako způsob přiřazení volbu **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 SystemB a heslo.
24. Klepnutím na tlačítko **OK** uložte profil PPP.

Aktivace pravidel paketů

Průvodce VPN automaticky vytvoří pravidla paketů, která toto připojení požaduje, aby pracovalo správně. Musíte je ale aktivovat v obou systémech ještě před připojením do VPN.

Chcete-li aktivovat pravidla paketů na systému A, proveďte tyto kroky:

1. V prostředí produktu System i Navigator rozbalte **Systém 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. Opakujte tento postup, chcete-li aktivovat pravidla paketů na systému B.

Scénář: Síť VPN vhodná pro bránu firewall

V tomto scénáři chce velká pojišťovací společnost vytvořit síť VPN mezi bránou v Chicagu a hostitelským systémem v Minneapolis, přičemž obě sítě jsou za bránou firewall.

Situace

Předpokládejme, že jste velká pojišťovací společnost sídlící v Minneapolis, která pojišťuje vlastníky domů a která právě otevřela novou pobočku v Chicagu. Pobočka v Chicagu potřebuje přístup k databázi v sídle společnosti v Minneapolis. Chcete zajistit bezpečnost přenášených informací, protože databáze obsahuje důvěrné informace o vašich zákaznících (například: jména, adresy a telefonní čísla). Rozhodli jste se propojit obě pobočky Internetem prostřednictvím sítě VPN (virtual private network). Obě pobočky jsou za bránou firewall a používají převod síťových adres (NAT), který umožňuje skrýt jejich neregistrované soukromé adresy IP za sadou registrovaných adres IP. Připojení VPN však mají některé dobře známé nekompatibility s převodem NAT. Připojení VPN vyřazuje pakety odesílané zařízením NAT, protože převod NAT mění adresu IP v paketu, a tím ho činí neplatným. Připojení VPN i tak můžete použít s převodem NAT, pokud implementujete zapouzdření UDP.

V tomto scénáři je soukromá adresa IP z chicagské sítě vložena do nového záhlaví protokolu IP a při průchodu bránou firewall C je přeložena (viz následující obrázek). Po přijetí paketu bránou firewall D přeloží brána firewall adresu IP cíle na adresu IP systému E. Paket proto bude předán na systém E. Systém E po přijetí tohoto paketu odstraní záhlaví UDP a ponechá původní paket IPSec, který pak projde všemi dalšími ověřeními platnosti, což umožní zabezpečené připojení VPN.

Cíle

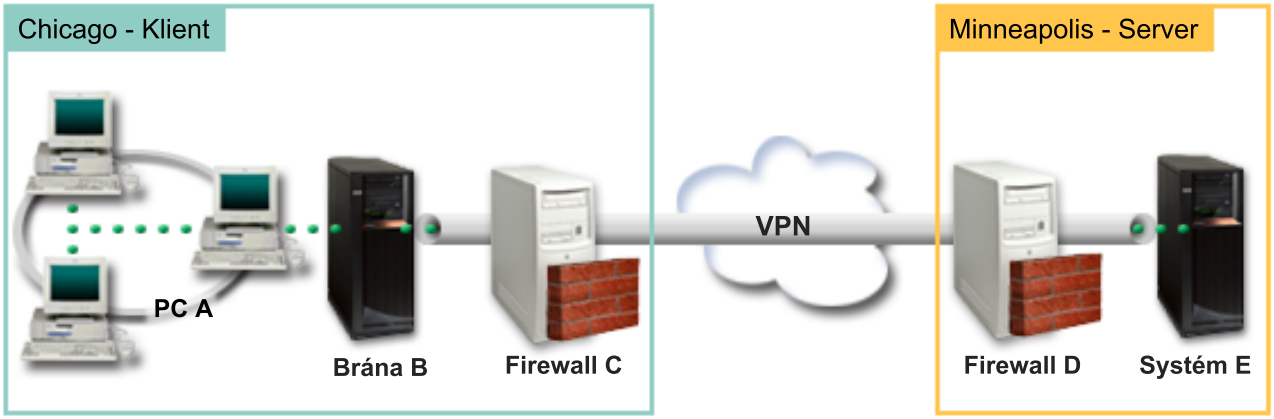
V tomto scénáři chce velká pojišťovací společnost vytvořit síť VPN mezi bránou v Chicagu (klient) a hostitelským systémem v Minneapolis (server), přičemž obě sítě jsou za bránou firewall.

Cíle tohoto scénáře:

- Brána pobočky v Chicagu vždy iniciuje připojení k hostiteli v Minneapolis.
- VPN musí chránit veškerý datový provoz mezi bránou v Chicagu a hostitelem v Minneapolis.
- Všichni uživatelé brány v Chicagu musí mít prostřednictvím VPN přístup k databázi serveru System i umístěné v minneapolisské síti.

Podrobnosti

Následující obrázek znázorňuje charakteristiku sítí pro tento scénář:



Chicagská síť - klient

- Komunikační brána B běží na operačním systému i5/OS verze 5, vydání 4 (V5R4) nebo novějším.
- Komunikační brána B se k Internetu připojuje pomocí adresy IP 214.72.189.35 a představuje přípojný a koncový bod tunelu VPN. Komunikační brána B provádí vyjednávání IKE a na odchozí datagramy protokolu IP používá zapouzdření UDP.
- Komunikační brána B a PC A jsou v podsíti 10.8.11.0 s maskou 255.255.255.0.
- PC A je zdrojem a cílem pro data procházející připojením VPN, jedná se proto o koncový bod tunelu VPN.
- Pouze komunikační brána B může iniciovat připojení k systému E.
- Brána firewall C má pravidlo Masq NAT s veřejnou adresou IP 129.42.105.17, která skrývá adresu IP komunikační brány B.

Minneapolisská síť - server

- Systém E běží na operačním systému i5/OS verze 5, vydání 4 (V5R4) nebo novějším.
- Systém E má adresu IP 56.172.1.1.
- Systém E je v tomto scénáři server, který odpovídá.
- Brána firewall D má adresu IP 146.210.18.51.
- Brána firewall D má statické pravidlo Static NAT, které mapuje veřejnou adresu IP (146.210.18.15) na soukromou adresu IP systému E (56.172.1.1). Z pohledu klientů se proto adresa IP systému E jeví jako veřejná adresa IP brány firewall D (146.210.18.51).

Úkoly konfigurace

Související pojmy

"Správa klíčů" na stránce 6
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.

"IPSec kompatibilní s převodem síťových adres (NAT) s UDP" na stránce 9
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.

Vyplnění pracovních formulářů pro plánování

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: Pro komunikační bránu B a systém E existují samostatné pracovní formuláře.

Tabulka 5. Systémové požadavky

Kontrolní seznam nezbytných předpokladů	**Odpovědi**
Je operační systém i5/OS V5R4 nebo novější?	Ano
Je nainstalována volba Digital Certificate Manager?	Ano
Je produkt System i Access for Windows nainstalovaný?	Ano
Je produkt System i Navigator nainstalovaný?	Ano
Je podkomponenta Síť produktu System i Navigator nainstalovaná?	Ano
Je produkt IBM TCP/IP Connectivity Utilities for i5/OS nainstalovaný?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano
Máte v systému 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 bránami firewall nebo směrovači, které používají filtrování IP paketů, podporují pravidla filtrování bran firewall a směrovačů protokoly AH a ESP?	Ano
Jsou brány firewall nebo směrovače nakonfigurovány tak, aby povolovaly provoz přes port 4500 pro vyjednávání klíče? Když protokol IKE zjistí, že jsou pakety NAT odesílány přes port 4500, partneři VPN obvykle provádějí vyjednávání výměny klíče (IKE) přes port UDP 500.	Ano
Jsou brány firewall konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Tabulka 6. Konfigurace komunikační brány B

Informace potřebné pro konfiguraci VPN pro komunikační bránu B	**Odpovědi**
Jaký typ připojení vytváříte?	od brány k jinému hostiteli
Jak pojmenujete skupinu dynamických klíčů?	CHIgw2MINhost
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu klíčů?	Vyvážený
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Ne: topsecretstuff
Jaký je identifikátor lokálního klíčového serveru?	Adresa IP: 214.72.189.35
Jaký je identifikátor lokálního datového koncového systému?	Podsíť: 10.8.11.0, maska: 255.255.255.0
Jaký je identifikátor vzdáleného klíčového serveru?	Adresa IP: 146.210.18.51
Jaký je identifikátor vzdáleného datového koncového systému?	Adresa IP: 146.210.18.51

Tabulka 6. Konfigurace komunikační brány B (pokračování)

Informace potřebné pro konfiguraci VPN pro komunikační bránu B	Odpovědi
Jaké porty a protokoly chcete povolit pro tok dat připojením?	Libovolné
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu dat?	Vyvážený
Na která rozhraní budou připojení použita?	TRLINE

Tabulka 7. Konfigurace systému E

Informace potřebné pro konfiguraci VPN pro systém E	Odpovědi
Jaký typ připojení vytváříte?	od hostitele k jiné bráně
Jak pojmenujete skupinu dynamických klíčů?	CHIgw2MINhost
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu klíčů?	Nejvyšší
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	Ne: topsecretstuff
Jaký je identifikátor lokálního klíčového serveru?	Adresa IP: 56.172.1.1
Jaký je identifikátor vzdáleného klíčového serveru? **Poznámka:** Je-li adresa IP brány firewall C neznámá, můžete jako identifikátor pro vzdálený klíčový server použít *ANYIP.	Adresa IP: 129.42.105.17
Jaký je identifikátor vzdáleného datového koncového systému?	Podsíť: 10.8.11.0, maska: 255.255.255.0
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

Související odkazy

Pomocný program pro plánování VPN

Konfigurace sítě VPN na komunikační bráně B

Chcete-li konfigurovat připojení k síti VPN na komunikační bráně B, proveďte následující kroky.

Použijte informace z pracovních formulářů a konfigurujte VPN na komunikační bráně B:

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 CHIgw2MINhost.
6. Volitelně zadejte popis této skupiny připojení.
7. Klepnutím na tlačítko **Další** přejděte na stranu **Scénář připojení**.
8. Vyberte **Připojit vaši komunikační bránu 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 **Vyvážené zabezpečení a výkon**.

    Poznámka: Zobrazí-li se chybová zpráva ″Požadavek certifikátu nelze provést″, můžete ji ignorovat, protože pro výměnu klíče nepoužíváte certifikáty.
11. Volitelné: Máte-li nainstalované certifikáty, zobrazí se stránka **Certifikát pro lokální koncový systém připojení**. Vyberte Ne, což znamená, že při autentizaci připojení budete používat certifikáty.
12. Klepnutím na tlačítko **Další** přejděte na stranu **Lokální klíčový server**.
13. V poli **Typ identifikátoru** vyberte **Adresa IP verze 4**.

14. V poli **Adresa IP** vyberte 214.72.189.35.
15. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený klíčový server**.
16. V poli **Typ identifikátoru** vyberte **Adresa IP verze 4**.
17. V poli **Identifikátor** vyberte 146.210.18.51.

    Poznámka: Komunikační brána B zahájí připojení na statický převod síťových adres. Chcete-li zadat jednotlivou adresu IP pro vzdálený klíč, musíte zadat výměnu klíče hlavního režimu. Výměna klíče hlavního režimu se vybere jako předvolená v případě, že připojení vytvoříte pomocí Průvodce připojením VPN. Použijete-li v této situaci agresivní režim, musíte pro vzdálený klíč zadat jiný typ vzdáleného identifikátoru než IPV4.
18. V poli **Předem nasdílený klíč** zadejte topsecretstuff.
19. Klepnutím na tlačítko **Další** přejděte na stranu **Lokální datový koncový systém**.
20. V poli **Typ identifikátoru** vyberte **Podsíť IP verze 4**.
21. V poli **Identifikátor** zadejte 10.8.0.0.
22. V poli **Maska podsítě** zadejte 255.255.255.0.
23. Klepnutím na tlačítko **Další** přejděte na stranu **Datové služby**.
24. Potvrďte předvolené hodnoty a potom klepnutím na tlačítko **Další** přejděte na stranu Zásada pro práci s daty.
25. Vyberte **Vytvořit novou zásadu** a potom vyberte **Vyvážené zabezpečení a výkon**.
26. Klepnutím na tlačítko **Další** přejděte na stranu **Rozhraní aplikací**.
27. V tabulce Linka vyberte **TRLINE**.
28. Klepnutím na tlačítko **Další** přejděte na stranu **Souhrn**.
29. Zkontrolujte, zda jsou průvodcem vytvořené objekty správné.
30. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci.
31. Když se zobrazí dialog **Aktivovat filtry zásad**, vyberte **Ano**, aktivujte vytvořené filtry zásad a potom vyberte **Povolit další přenosy**.
32. Klepnutím na tlačítko **OK** dokončete konfiguraci.

Konfigurace sítě VPN na systému E

Chcete-li konfigurovat připojení k síti VPN na systému E, proveďte následující kroky:

Použijte informace z pracovních formulářů a konfigurujte VPN na systému E:

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 CHIgw2MINhost.
6. Volitelně zadejte popis této skupiny připojení.
7. Klepnutím na tlačítko **Další** přejděte na stranu **Scénář připojení**.
8. Vyberte **Připojit vašeho hostitele 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**.

    Poznámka: Zobrazí-li se chybová zpráva ″Požadavek certifikátu nelze provést″, můžete ji ignorovat, protože pro výměnu klíče nepoužíváte certifikáty.
11. Volitelné: Máte-li nainstalované certifikáty, zobrazí se stránka **Certifikát pro lokální koncový systém připojení**. Vyberte Ne, což znamená, že při autentizaci připojení budete používat certifikáty.
12. Klepnutím na tlačítko **Další** přejděte na stranu **Lokální klíčový server**.

13. V poli **Typ identifikátoru** vyberte **Adresa IP verze 4**.
14. V poli **Adresa IP** vyberte 56.172.1.1.
15. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený klíčový server**.
16. V poli **Typ identifikátoru** vyberte **Adresa IP verze 4**.
17. V poli **Identifikátor** vyberte 129.42.105.17.

    Poznámka: Je-li adresa IP brány firewall C neznámá, můžete jako identifikátor pro vzdálený klíčový server použít *ANYIP.
18. V poli **Předem nasdílený klíč** zadejte topsecretstuff.
19. Klepnutím na tlačítko **Další** přejděte na stranu **Vzdálený datový koncový systém**.
20. V poli **Typ identifikátoru** vyberte **Podsíť IP verze 4**.
21. V poli **Identifikátor** vyberte 10.8.11.0.
22. V poli **Maska podsítě** zadejte 255.255.255.0.
23. Klepnutím na tlačítko **Další** přejděte na stranu **Datové služby**.
24. Potvrďte předvolené hodnoty a potom klepnutím na tlačítko **Další** přejděte na stranu Zásada pro práci s daty.
25. Vyberte **Vytvořit novou zásadu** a potom vyberte **Vyvážené zabezpečení a výkon**.
26. Klepnutím na tlačítko **Další** přejděte na stranu **Rozhraní aplikací**.
27. V tabulce Linka vyberte **TRLINE**.
28. Klepnutím na tlačítko **Další** přejděte na stranu **Souhrn**.
29. Zkontrolujte, zda jsou průvodcem vytvořené objekty správné.
30. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci.
31. Když se zobrazí dialog **Aktivovat filtry zásad**, vyberte **Ano**, aktivujte vytvořené filtry zásad a potom vyberte **Povolit další přenosy**.
32. Klepnutím na tlačítko **OK** dokončete konfiguraci.

Spuštění připojení

Poté, co jste nakonfigurovali připojení VPN na systému E, musíte připojení VPN spustit.

Pomocí následujícího postupu ověřte, zda je připojení CHIgw2MINhost na systému E aktivní:

1. V prostředí produktu System i Navigator rozbalte **Systém E → Síť → Zabezpečená připojení → Všechna připojení**.
2. Podívejte se na připojení **CHIgw2MINhost** a ověřte, zda je v poli **Stav** hodnota *Nečinné* nebo *Na vyžádání*.

Chcete-li navázat připojení CHIgw2MINhost z komunikační brány B, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Komunikační brána B → Síť → Zásady pro práci s IP**.
2. Není-li server VPN spuštěn, klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**.
3. Rozbalte **VPN → Zabezpečená připojení**.
4. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
5. Klepněte pravým tlačítkem na **CHIgw2MINhost** a vyberte **Spustit**.
6. V menu **Zobrazení** vyberte příkaz **Obnovit**. Je-li připojení úspěšně spuštěno, změní se **Stav** z hodnoty *Probíhá spuštění* nebo *Na vyžádání* na *Aktivní*. Spuštění připojení může trvat nějakou dobu, proto pravidelně aktualizujte, dokud se stav nezmění na *Aktivní*.

Testování připojení

Po dokončení konfigurování komunikační brány B a systému E a úspěšném spuštění serverů VPN otestujte připojitelnost, aby bylo zajištěno, že oba systémy spolu mohou komunikovat.

Chcete-li testovat připojení, postupujte takto:

1. V síti PC A vyhledejte systém a spusťte relaci Telnet.

2. Pro systém E zadejte veřejnou adresu IP 146.210.18.51.
3. Je-li to třeba, zadejte přihlašovací informace. Pokud se zobrazí přihlašovací obrazovka, připojení funguje.

Scénář: Připojení sítě VPN ke vzdáleným uživatelům

Administrátor musí nakonfigurovat připojení sítě VPN ke vzdáleným uživatelům a povolit vzdálená připojení.

Následující úlohy vám ukazují, jak administrátor konfiguruje připojení sítě VPN ke vzdáleným uživatelům.

Vyplnění plánovacích pracovních formulářů pro připojení k VPN z pobočky ke vzdáleným obchodním zástupcům

Administrátor pobočky používá poradce při plánování VPN k vytvoření dynamických plánovacích pracovních formulářů pro pomoc při konfiguraci sítě VPN na systémech a vzdálených pracovních stanicích.

Poradce při plánování sítě VPN je interaktivní nástroj, který pokládá určité otázky ohledně potřeb VPN. Podle vašich odpovědí poradce vygeneruje přizpůsobený plánovací pracovní formulář pro dané prostředí, který můžete použít ke konfiguraci připojení k síti VPN. Tento pracovní formulář lze pak použít ke konfiguraci VPN na systému. Každý z následujících plánovacích pracovních formulářů je generován s pomocí poradce pro plánování sítě VPN a použije se ke konfiguraci VPN s pomocí průvodce novým připojením VPN v produktu System i Navigator.

Tabulka 8. Plánovací pracovní formulář pro připojení k síti VPN mezi pobočkou a vzdálenými obchodními zástupci

Na co se ptá průvodce VPN	**Co poradce VPN doporučí**
Jak se bude nazývat tato skupina připojení?	SalestoRemote
Jaký typ skupiny připojení chcete vytvořit?	Vyberte **Připojit hostitele k jinému hostiteli**.
Jakou zásadu vzájemné výměny klíčů po Internetu chcete použít pro ochranu klíče?	Vyberte **Vytvořit novou zásadu** a potom vyberte **Nejvyšší zabezpečení, nejnižší výkon**.
Používáte certifikáty?	Vyberte **Ne**.
Zadejte identifikátor, který bude znázorňovat lokální server klíčů pro toto připojení.	Typ identifikátoru: **Adresa IP verze 4**, Adresa IP:**192.168.1.2**. Pro adresu IPv6 je typ identifikátoru: **Adresa IP verze 6**, Adresa IP:**2001:DB8::2** **Poznámka:** Adresy IP použité v tomto scénáři jsou uvedeny jen jako příklad. Neodrážejí schéma adresování IP a neměly by se použít v žádné skutečné konfiguraci. Při provádění těchto úloh byste měli používat vlastní adresy IP.
Jaký je identifikátor klíčového serveru, k němuž se chcete připojit?	Typ identifikátoru: **Libovolná adresa IP**, **Předem sdílený klíč**: mycokey. **Poznámka:** Předem sdílený klíč je 32znakový textový řetězec, který i5/OS VPN používá k ověření připojení a k zavedení klíčů, které chrání vaše data. Obecně byste s ním měli zacházet stejně jako s heslem.
Jaké jsou porty a protokoly dat, které bude toto připojení chránit?	**Lokální port**: 1701, **Vzdálený port**: Libovolný port, **Protokol**: UDP

Tabulka 8. Plánovací pracovní formulář pro připojení k síti VPN mezi pobočkou a vzdálenými obchodními zástupci (pokračování)

Na co se ptá průvodce VPN	Co poradce VPN doporučí
Jakou zásadu pro práci s daty chcete použít k ochraně dat?	Vyberte **Vytvořit novou zásadu** a potom vyberte **Nejvyšší zabezpečení, nejnižší výkon**.
Zkontrolujte rozhraní na lokálním systému, na který se toto připojení použije.	ETHLINE (pobočka)

Konfigurace profilu terminátoru L2TP pro systém A

Chcete-li konfigurovat vzdálená připojení ke vzdáleným pracovním stanicím, budete muset nastavit systém A, aby přijímal příchozí připojení od těchto klientů.

Chcete-li konfigurovat profil terminátoru L2TP (Layer Two Tunneling Protocol) pro systém A, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***Systém A*** → **Síť** → **Služby vzdáleného přístupu**.
2. Klepněte pravým tlačítkem myši na **Profily připojení příjemce**, abyste mohli nastavit systém A jako server, který umožňuje příchozí připojení vzdálených uživatelů, a vyberte **Nový profil**.
3. V menu nastavení stránky vyberte následující volby:
   - **Typ protokolu:** PPP
   - **Typ připojení:** L2TP (virtuální linka)

     Poznámka: V poli **Provozní režim** by se měl automaticky zobrazit **Terminátor (síťový server)**.
   - **Typ služby linky:** jediná linka
4. Klepněte na tlačítko **OK**. Zobrazí se stránka Vlastnosti nového profilu dvoubodového spojení.
5. Na kartě **Obecné** dokončete nastavení následujících polí:
   - **Jméno**: MYCOL2TP
   - Vyberte **Spustit profil s TCP**, pokud chcete profil spustit automaticky s TCP.
6. Na kartě **Připojení** vyberte **192.168.1.2** (**2001:DB8::2** v IPv6) pro **adresu IP koncového bodu lokálního tunelu**.

   Důležité: Adresy IP použité v tomto scénáři jsou uvedeny jen jako příklad. Neodrážejí schéma adresování IP a neměly by se použít v žádné skutečné konfiguraci. Při provádění těchto úloh byste měli používat vlastní adresy IP.
7. Vyberte **MYCOL2TP** jako **Jméno virtuální linky**. Zobrazí se stránka Vlastnosti nového profilu L2TP.
8. Na stránce Autentizace zadejte systema jako jméno hostitele. Klepněte na tlačítko **OK**. Vrátíte se na stránku připojení.
9. Na stránce Připojení vyberte následující volby a zadejte 25 jako **Maximální počet připojení**.
   a. Klepněte na kartu **Autentizace** a vyberte volbu **Požadovat, aby tento systém ověřil identitu vzdáleného systému**.
   b. Vyberte volbu **Lokální autentizace pomocí ověřovacího seznamu**.
   c. Zadejte QL2TP do pole **Jméno ověřovacího seznamu** a klepněte na **Nový**.
10. Na stránce Ověřovací seznam vyberte **Přidat**.
11. Přidejte jména uživatelů a hesla pro vzdálené pracovníky. Klepněte na tlačítko **OK**.
12. Na stránce Potvrzení hesla znovu zadejte heslo pro každého vzdáleného pracovníka. Klepněte na tlačítko **OK**.
13. Na stránce Nastavení TCP/IP vyberte 10.1.1.1 (2001:DA8::1 v IPv6) jako **Lokální adresu IP**.
14. V poli **Metoda přiřazení adresy IP** vyberte **Oblast adres**.
15. V poli **Počáteční adresa IP** zadejte 10.1.1.100 a 49jako **Počet adres**. U adresy IPv6 zadejte v poli **Počáteční adresa IP** 2001:DA8::1:1 a 65535 jako **Počet adres**.
16. Vyberte **Povolit vzdálenému systému přístup k dalším sítím (přesměrování IP)**. Klepněte na tlačítko **OK**.

Spuštění profilu připojení příjemce

Poté, co nakonfigurujete profil připojení L2TP (Layer Two Tunneling Protocol) pro systém A, administrátor musí toto připojení spustit, aby naslouchalo příchozím požadavkům od vzdálených klientů.

Poznámka: Možná obdržíte chybovou zprávu, že subsystém QUSRWRK nebyl spuštěn. Tato zpráva se vyskytne při pokusu o spuštění profilu připojení příjemce. Chcete-li spustit subsystém QUSRWRK, postupujte takto:

1. Ve znakově orientovaném rozhraní zadejte strsbs.
2. Na obrazovce Spuštění subsystému zadejte QUSRWRK do pole **Popis subsystému**.

Chcete-li spustit profil připojení příjemce pro vzdálené klienty, proveďte tyto úlohy:

1. V prostředí produktu System i Navigator vyberte **Obnovit** v nabídce **Zobrazení**. Tak obnovíte instanci produktu System i Navigator.
2. V prostředí produktu System i Navigator rozbalte ***Systém A*** **→ Síť → Služby vzdáleného přístupu**.
3. Poklepejte na **Profily připojení příjemce** a klepněte pravým tlačítkem myši na **MYCOL2TP** a vyberte **Spustit**.
4. Zobrazí se pole **Stav**, **Čeká na požadavky na připojení**.

Konfigurace připojení k síti VPN na systému A pro vzdálené klienty

Poté, co pro systém A nakonfigurujete profil připojení příjemce L2TP (Layer Two Tunneling Protocol), administrátor musí nakonfigurovat síť VPN pro ochranu připojení mezi vzdálenými klienty a sítí v kanceláři pobočky.

Chcete-li konfigurovat síť VPN pro vzdálené klienty, postupujte takto:

Důležité: Adresy IP použité v tomto scénáři jsou uvedeny jen jako příklad. Neodrážejí schéma adresování IP a neměly by se použít v žádné skutečné konfiguraci. Při provádění těchto úloh byste měli používat vlastní adresy IP.

1. V prostředí produktu System i Navigator rozbalte ***Systém 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 sítě VPN. Informace o tom, které objekty průvodce vytváří, najdete na straně Vítejte.
3. Klepnutím na tlačítko **Další** přejdete na stranu Jméno připojení.
4. Do pole **Jméno** zadejte SalestoRemote.
5. Volitelné: Zadejte popis této skupiny připojení. Klepněte na **Další**.
6. Na stránce Scénář připojení vyberte **Připojit hostitele k jinému hostiteli**. Klepněte na **Další**
7. Na stránce Zásady výměny klíčů po Internetu vyberte **Vytvořit novou zásadu** , a pak vyberte **Nejvyšší zabezpečení, nejnižší výkon**. Klepněte na **Další**.
8. Na stránce Certifikát pro koncový bod lokálního připojení vyberte **Ne**. Klepněte na **Další**.
9. Na stránce Lokální server klíčů vyberte **Adresa IP verze 4** jako typ identifikátoru. Přidružená adresa IP by měla být 192.168.1.2. Klepněte na **Další**. Pro adresu IPv6 na stránce Lokální server klíčů vyberte **Adresa IP verze 6** jako typ identifikátoru. Přidružená adresa IP by měla být 2001:DB8::2. Klepněte na **Další**.
10. Na stránce Vzdálený server klíčů vyberte **Libovolná adresa IP** v poli **Typ identifikátoru**. Do pole **Předem sdílený klíč** zadejte mycokey. Klepněte na **Další**.
11. Na stránce Datové služby zadejte 1701 jako lokální port. Pak vyberte 1701 jako vzdálený port a vyberte **UDP** jako protokol. Klepněte na **Další**.
12. Na stránce Zásady pro práci s daty vyberte **Vytvořit novou zásadu** , a pak vyberte **Nejvyšší zabezpečení, nejnižší výkon**. Klepněte na **Další**.
13. Na stránce Použitelná rozhraní vyberte **ETHLINE**. Klepněte na **Další**.
14. Na stránce Souhrn zobrazte objekty vytvořené průvodcem a ujistěte se, že jsou správné.
15. Klepnutím na tlačítko **Dokončit** dokončete konfiguraci. Když se zobrazí okno Aktivovat filtry zásad, vyberte **Ne, pravidla paketů budou aktivována později**. Klepněte na tlačítko **OK**.

Aktualizace zásad VPN pro vzdálená připojení z klientů Windows XP a Windows 2000

Protože průvodce vytvoří standardní připojení, které lze použít pro většinu konfigurací sítě VPN (virtual private network), budete muset aktualizovat zásady generované průvodcem, abyste zajistili interoperabilitu s klienty systému Windows XP a Windows 2000.

Chcete-li aktualizovat tyto zásady VPN, proveďte následující úlohy:

1. V prostředí produktu System i Navigator rozbalte ***Systém A*** → **Síť** → **Zásady pro práci s IP** → **VPN** → **Zásady zabezpečení IP**.
2. Poklepejte na **Zásady vzájemné výměny klíčů přes Internet** a klepněte pravým tlačítkem myši na **Libovolná adresa IP** a vyberte **Vlastnosti**.
3. Na stránce Transform klepněte na **Přidat**.
4. Na stránce Přidat transform pro vzájemnou výměnu klíčů přes Internet vyberte následující volby:
   - **Metoda autentizace:** předem sdílený klíč
   - **Hašovací algoritmus:** MD5
   - **Šifrovací algoritmus:** DES-CBC
   - **Skupina Diffie-Hellmana:** skupina 1
5. Klepněte na tlačítko **OK**.
6. V prostředí produktu System i Navigator rozbalte ***Systém A*** → **Síť** → **Zásady pro práci s IP** → **VPN** → **Zásady zabezpečení IP**.
7. Poklepejte na **Zásady pro práci s daty** a klepněte pravým tlačítkem myši na **SalestoRemote** a vyberte **Vlastnosti**.
8. Na stránce Obecné vyčistěte **Použít úplné utajení přesměrování Diffie-Hellman**.
9. Vyberte **Návrh ESP**, klepněte na **Upravit**.
10. Na stránce Návrh zásady pro práci s daty upravte volby následujícím způsobem:
    - **Režim zapouzdření:** přenos
    - **Ukončení platnosti klíče:** 15 minut
    - **Velikostní limit pro ukončení platnosti:** 100000
11. Na stránce Transform klepněte na **Přidat**.
12. Na stránce Přidat transform zásady pro práci s daty vyberte následující volby:
    - **Protokol:** ESP (Encapsulating security payload)
    - **Autentizační algoritmus:** MD5
    - **Šifrovací algoritmus:** DES-CBC
13. Dvakrát klepněte na tlačítko **OK**.

Aktivace pravidel filtrování

Průvodce automaticky vytvoří pravidla paketů, která toto připojení požaduje, aby pracovalo správně. Musíte je ale aktivovat v obou systémech ještě před připojením do VPN.

Chcete-li aktivovat pravidla filtrování na systému A, proveďte tyto kroky:

Důležité: Adresy IP použité v tomto scénáři jsou uvedeny jen jako příklad. Neodrážejí schéma adresování IP a neměly by se použít v žádné skutečné konfiguraci. Při provádění těchto úloh byste měli používat vlastní adresy IP.

1. V prostředí produktu System i Navigator rozbalte ***Systém A*** → **Síť** → **Zásady pro práci s IP**.
2. Klepněte pravým tlačítkem na **Pravidla paketů** a vyberte **Aktivovat pravidla**.
3. Na stránce Aktivace pravidel paketů vyberte **aktivovat pouze pravidla generovaná VPN** a vyberte **ETHLINE** jako rozhraní, kde byste chtěli aktivovat tato pravidla filtrování. Klepněte na tlačítko **OK**.

Než budou moci vzdálení uživatelé konfigurovat pracovní stanice Windows XP, administrátor jim dá následující informace pro nastavení připojení na jejich straně. Každému ze vzdálených uživatelů poskytněte tyto informace:

- jméno předem sdíleného klíče: mycokey
- adresa IP systému A: 192.168.1.2 (2001:DB8::2 v IPv6)
- jméno uživatele a heslo pro připojení

Poznámka: Byly vytvořeny, když uživatel přidal jméno uživatele a hesla na ověřovací seznam při konfiguraci profilu terminátoru L2TP (Layer Two Tunneling Protocol).

Konfigurace VPN na klientovi Windows XP

Použijte tuto proceduru pro konfiguraci VPN na klientovi Windows XP.

Vzdálení uživatelé MyCo, Inc musí nastavit vzdáleného klienta Windows XP s pomocí těchto kroků:

1. V systému Windows XP v nabídce **Start** rozbalte **Všechny programy → Příslušenství → Komunikace → Průvodce novým připojením**.
2. Na úvodní stránce si přečtěte souhrnné informace. Klepněte na **Další**.
3. Na stránce Typ připojení do sítě vyberte **Připojit do sítě v mojí pracovní oblasti**. Klepněte na **Další**.
4. Na stránce Připojení do sítě vyberte **Připojení do sítě VPN (Virtual Private Network)**. Klepněte na **Další**.
5. Na stránce Jméno připojení zadejte Připojení k filiálce v poli **Jméno společnosti**. Klepněte na **Další**.
6. Na stránce Veřejná síť vyberte **Nevytáčet počáteční připojení**. Klepněte na **Další**.
7. Na stránce Výběr serveru VPN zadejte 192.168.1.2 (2001:DB8::2 v IPv6) do pole **Jméno hostitele nebo adresa IP**. Klepněte na **Další**.
8. Na stránce Dostupnost připojení vyberte **Pouze pro moje použití**. Klepněte na **Další**.
9. Na stránce Souhrn klepněte na **Přidat zástupce tohoto připojení na pracovní plochu**. Klepněte na tlačítko **Dokončit**.
10. Klepněte na ikonu **Připojit k MyCo**, která byla vytvořena na pracovní ploše.
11. Na stránce Připojení k MyCo zadejte jméno uživatele a heslo, které poskytnul administrátor.
12. Vyberte **Uložit toto jméno uživatele a heslo pro následující uživatele** a **Pouze já**. Klepněte na **Vlastnosti**.
13. Na stránce **Zabezpečení** se ujistěte, že jsou vybrány následující **Volby zabezpečení**:
    - **Typické**
    - **Požadovat bezpečnostní heslo**
    - **Požadovat šifrování dat**

    Klepněte na **Nastavení IPSec**.
14. Na stránce Nastavení IPSec vyberte **Použít předem sdílený klíč pro autentizaci** a zadejte mycokey do pole **Předem sdílený klíč**. Klepněte na tlačítko **OK**.
15. Na stránce Připojení do sítě vyberte **L2TP IPSec VPN** jako **Typ sítě VPN**. Klepněte na tlačítko **OK**.
16. Přihlaste se se jménem uživatele a heslem a klepněte na **Připojit**.

Chcete-li spustit připojení do sítě VPN (virtual private network) na straně klienta, klepněte na ikonu, která se objeví na pracovní ploše poté, co dokončíte průvodce připojením.

Testování připojení k VPN mezi koncovými body

Po dokončení konfigurace připojení mezi systémem A a vzdálenými uživateli a úspěšném spuštění připojení byste měli otestovat připojitelnost, abyste se ujistili, že vzdálení hostitelé spolu mohou komunikovat.

Chcete-li testovat připojení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte ***Systém A*** **→ Síť**.
2. Klepněte pravým tlačítkem na **Konfigurace TCP/IP** a vyberte **Obslužné programy** a potom vyberte **Testovat spojení**.

3. V dialogu **Testovat spojení z** zadejte 10.1.1.101 (2001:DA8::1:101 v IPv6) do pole **Testování spojení**.

   Poznámka: 10.1.1.101 znázorňuje dynamicky přiřazenou adresu IP (ke vzdálenému obchodnímu klientovi) z oblasti adres uvedeného v profilu terminátoru L2TP (Layer Two Tunneling Protocol) na systému A.
4. Klepnutím na tlačítko **Testovat spojení ihned** ověřte připojitelnost ze systému A na vzdálenou pracovní stanici. Klepněte na tlačítko **OK**.

Při testování spojení ze vzdáleného klienta zaměstnanec na vzdáleném systému provede tyto kroky na stanici, kde běží operační systém Windows:

1. V příkazovém řádku zadejte ping 10.1.1.2 (ping 2001:DA8::2 v protokolu IPv6). To bude adresa IP jedné z pracovních stanic v síti na ústředí.
2. Zopakujte tyto kroky pro testování propojitelnosti z ústřední kanceláře k filiálce.

Scénář: Použití převodu síťových adres pro VPN

V tomto scénáři si chce vaše společnost vyměňovat citlivá data s jedním z obchodních partnerů pomocí připojení VPN. K další ochraně soukromých údajů své síťové struktury použije společnost také převod síťových adres VPN (VPN NAT), aby skryla soukromou adresu IP systému, který používá jako hostitelský systém aplikací, ke kterým má obchodní partner přístup.

Situace

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 ručně, 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 adresy IP systému, který je hostitelem aplikací, k nimž má mít dodavatel přístup.

VPN můžete použít nejen k vytvoření definic připojení v komunikační bráně VPN v podnikové síti, ale také k provádění převodu adres, abyste mohli skrýt lokální soukromé adresy. Na rozdíl od konvenčního převodu síťových adres (NAT), který změní adresy IP v přidruženích zabezpečení (VPN ale vyžaduje, aby tyto adresy IP byly funkční), provádí VPN NAT převod adres před ověřením platnosti přidružení zabezpečení tím, že adresu přiřadí k připojení, když se toto připojení spustí.

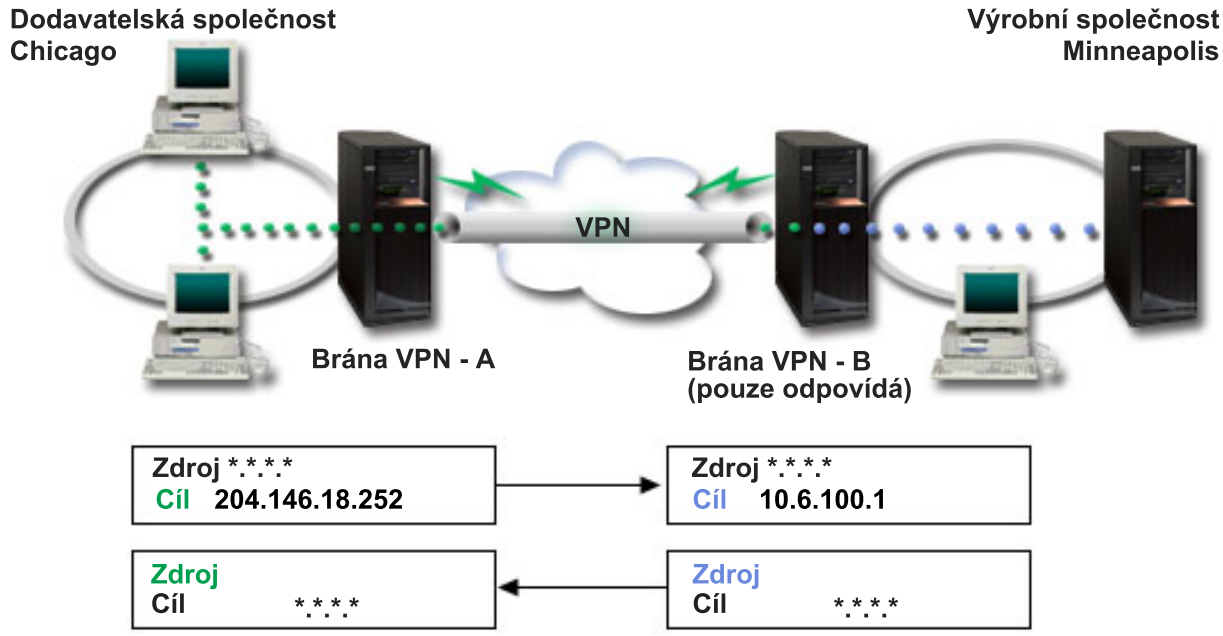
Cíle

Cíle tohoto scénáře:

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

Podrobnosti

Následující diagram znázorňuje síťovou charakteristiku sítě dodavatele i sítě výrobce:



- Komunikační brána VPN - A je konfigurována tak, aby vždy iniciovala připojení do komunikační brány VPN - B.
- Komunikační brána VPN - A určuje cílový koncový systém pro připojení jako 204.146.18.252 (veřejná adresa přiřazená systému C).
- Soukromá adresa IP systému C v síti výrobce je 10.6.100.1.
- Veřejná adresa 204.146.18.252 byla definována v lokální oblasti služeb v komunikační bráně VPN - B pro soukromou adresu systému C, 10.6.100.1.
- Komunikační brána VPN - B převede veřejnou adresu systému C pro příchozí datagramy na soukromou adresu 10.6.100.1. Komunikační brána VPN - B převede vrácené odchozí datagramy z adresy 10.6.100.1 zpět na veřejnou adresu systému C, 204.146.18.252. Pokud jde o klienty v síti dodavatele, má systém C adresu IP 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 - A** a **VPN - B**.
2. Určení lokální oblasti služeb v komunikační bráně **VPN - B** pro skrytí soukromých adres **Systému C** do veřejného identifikátoru 204.146.18.252.
3. Konfigurace komunikační brány **VPN - B** pro převod lokálních adres pomocí adres z lokální oblsti služeb.

Související pojmy

“Převod síťových adres pro VPN” na stránce 8
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.

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.

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

- požadavky na nastavení VPN
- určení typu VPN
- 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 ručních připojení používejte pracovní formulář.
- Vyplnění pracovních formulářů pro plánování VPN

Až dokončíte plánování pro VPN, můžete začít s konfigurováním.

Související úlohy

Použití poradce při plánování VPN

“Konfigurace VPN” na stránce 45
Rozhraní VPN umožňuje několik různých způsobů konfigurace připojení VPN. Můžete konfigurovat ruční nebo dynamické připojení.

Požadavky na nastavení VPN

Aby připojení k síti VPN řádně fungovalo na systémech a s klienty sítě, musíte splňovat minimální požadavky.

V následujícím seznamu jsou uvedeny minimální požadavky na nastavení připojení k VPN:

Systémové požadavky

- Operační systém i5/OS verze 5, vydání 3, nebo novější.
- Digital Certificate Manager
- System i Access for Windows
- System i Navigator
  - Síťová komponenta produktu System i 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 řádně připojená k systému a nakonfigurovaná pro protokol TCP/IP.
- Základní jednotka 233 MHz.
- 32 MB RAM pro klienty operačního systému pro Windows 95.
- 64 MB RAM pro klienty operačního systému Windows NT 4.0 a Windows 2000.
- V PC klienta nainstalované produkty System i Access for Windows a System i Navigator.
- Software podporující protokol IPSec (IP Security).
- Software podporující protokol L2TP, pokud budou vzdálení uživatelé protokol L2TP používat při vytváření připojení s vaším systémem.

Související úlohy

“Začínáme s odstraňováním problémů s VPN” na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

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.

Zpracování pracovních formulářů plánování VPN

Pracovní formuláře VPN vám pomohou shromáždit podrobné údaje o plánech na využití VPN. Tyto formuláře je třeba vyplnit, chcete-li adekvátně plánovat strategii VPN. Můžete je také použít při konfigurování VPN.

Pracovní formuláře můžete vytisknout a vyplnit. Shromáždíte tak podrobné údaje o plánech na využití VPN.

Vyberte pracovní formulář pro typ připojení, který chcete vytvořit.

- pracovní formulář pro plánování dynamických připojení
- pracovní formulář pro ruční připojení
- pomocný program pro 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 ručních 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**.

Související informace

Pracovní formulář pro plánování dynamických připojení

Vyplňte tento pracovní formulář ještě před konfigurováním dynamického 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.

Tabulka 9. Systémové požadavky

Kontrolní seznam nezbytných předpokladů	**Odpovědi**
Je operační systém i5/OS V5R3 nebo novější?	Ano
Je nainstalována volba Digital Certificate Manager?	Ano
Je produkt System i Access for Windows nainstalovaný?	Ano
Je produkt System i Navigator nainstalovaný?	Ano
Je podkomponenta Síť produktu System i Navigator nainstalovaná?	Ano
Je produkt IBM TCP/IP Connectivity Utilities for i5/OS nainstalovaný?	Ano
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	Ano
Máte v systému 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 bránami firewall nebo směrovači, které používají filtrování IP paketů, podporují pravidla filtrování bran firewall a směrovačů protokoly AH a ESP?	Ano
Jsou brány firewall nebo směrovače konfigurovány tak, že povolují protokoly IKE (UDP port 500), AH a ESP?	Ano
Jsou brány firewall konfigurovány tak, že umožňují směrování pomocí IP?	Ano

Tabulka 10. Konfigurace VPN

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 • Zabezpečení a výkon Balance • Nejnižší zabezpečení, nejvyšší výkon	
Používáte certifikáty, chcete-li autentizovat připojení? Pokud ne, jaký je předem nasdílený klíč?	
Jaký je identifikátor lokálního klíčového serveru?	

Tabulka 10. Konfigurace VPN (pokračování)

Jaký je identifikátor lokálního klíčového serveru?	
Jaký je identifikátor vzdáleného klíčového serveru?	
Jaký je identifikátor vzdáleného datového koncového systému?	
Jaký typ zabezpečení a provozu vyžadujete v systému pro ochranu dat? • Nejvyšší zabezpečení, nejnižší výkon • Zabezpečení a výkon Balance • Nejnižší zabezpečení, nejvyšší výkon	

Pracovní formulář pro ruční připojení

Vyplňte tento pracovní formulář ještě před konfigurováním ručního 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:

Tabulka 11. Systémové požadavky

Kontrolní seznam nezbytných předpokladů	**Odpovědi**
Běží na systému operační systém i5/OS V5R3 nebo novější?	
Je nainstalován produkt Digital Certificate Manager?	
Je produkt System i Access for Windows nainstalovaný?	
Je produkt System i Navigator nainstalovaný?	
Je podkomponenta Síť produktu System i Navigator nainstalovaná?	
Je produkt IBM TCP/IP Connectivity Utilities for i5/OS nainstalovaný?	
Nastavili jste systémovou hodnotu QRETSVRSEC *SEC (retain server security) na hodnotu 1?	
Máte v systému konfigurován protokol TCP/IP (včetně rozhraní protokolu IP, přenosových cest, jména lokálního hostitelského systému a jména lokální domény)?	
Je mezi požadovanými koncovými systémy zavedena normální komunikace prostřednictvím protokolu TCP/IP?	
Provedli jste nejnovější opravy PTF?	
Jestliže tunel VPN prochází bránami firewall nebo směrovači, které používají filtrování IP paketů, podporují pravidla filtrování bran firewall a směrovačů protokoly AH a ESP?	
Jsou brány firewall nebo směrovače konfigurovány tak, že povolují protokoly AH a ESP?	
Jsou brány firewall konfigurovány tak, že umožňují směrování pomocí IP?	

Tabulka 12. Konfigurace VPN

Informace potřebné pro konfiguraci ručního 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?	

Tabulka 12. Konfigurace VPN (pokračování)

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.	
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.	

Související pojmy

“Převod síťových adres pro VPN” na stránce 8
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.

Konfigurace VPN

Rozhraní VPN umožňuje několik různých způsobů konfigurace připojení VPN. Můžete konfigurovat ruční nebo dynamické připojení.

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.

Ruční 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. Ruční připojení používají statické klíče, které nelze obnovit ani měnit, dokud je připojení aktivní. Ruční připojení musíte ukončit, chcete-li změnit jeho přidružený klíč. Pokud toto považujete za bezpečnostní riziko, můžete místo ručního připojení vytvořit dynamické.

Související pojmy

"Plán pro VPN" na stránce 41
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 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 prostředí produktu System i Navigator rozbalte **Systém → 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**.

Související úlohy

Pomocný program pro plánování VPN

Konfigurace zásad zabezpečení VPN

Až určíte, jak budete VPN používat, musíte definovat zásady zabezpečení VPN.

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

Související úlohy

"Konfigurace zabezpečeného připojení VPN" na stránce 48
Až dokončíte konfiguraci zásad zabezpečení, musíte konfigurovat zabezpečené připojení.

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 ruční připojení, nemusíte zásadu IKE definovat. Vytváříte-li VPN pomocí průvodce novým připojením, průvodce může zásadu IKE vytvořit za vás.

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 Digital Certificate Manager. 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 prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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.

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. Chcete-li při výměně klíčů vynutit použití vyjednávání v hlavním režimu, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP**.
2. Chcete-li prohlížet aktuálně definované zásady výměny klíčů v pravém podokně, vyberte **VPN (Virtual Private Networking) → Zásady zabezpečení IP → Metody IKE (Internet Key Exchange)**.
3. Klepněte pravým tlačítkem na určitou zásadu výměny klíčů a vyberte **Vlastnosti**.
4. Na straně Transformy klepněte na **Odpovídající zásada**. Objeví se dialog Odpovídající zásada IKE (Internet Key Exchange).
5. V poli Ochrana identity zrušte vybrání volby **Vyjednávání IKE v agresívním režimu (bez ochrany identity)**.
6. Klepnutím na tlačítko **OK** se vraťte do dialogu Vlastnosti.
7. Opětovným klepnutím na tlačítko **OK** uložte provedené změny.

Poznámka: Když nastavíte pole ochrany identity, bude změna platná pro všechny výměny se vzdálenými klíčovými servery, protože v celém systému existuje pouze jedna zásada IKE pro odpovídající stranu. Vyjednávání v hlavním režimu zajišťuje, že iniciátor může požadovat pouze zásadu IKE v hlavním režimu.

Související pojmy

“Správa klíčů” na stránce 6

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.

Související úlohy

DCM (Digital Certificate Manager)

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). Když vytváříte ruční 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.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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.

Související pojmy

"Správa klíčů" na stránce 6
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.

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 přidruženy k pravidlu filtrování zásad s typem akce IPSEC. Pokud specifické datové koncové systémy nabídnuté vzdáleným iniciátorem jsou v rozsahu určeném pravidlem filtrování 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 nakonfigurovat objekt zabezpečeného připojení, proveďte úkoly části 1 i 2:

Související pojmy

"Konfigurace zásad zabezpečení VPN" na stránce 46
Až určíte, jak budete VPN používat, musíte definovat zásady zabezpečení VPN.

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Související úlohy

"Aktivace pravidel paketů VPN" na stránce 54
Před spuštěním vlastních připojení VPN musíte aktivovat pravidla paketů VPN.

Část 1: Konfigurace skupiny s dynamicky přiřazeným klíčem

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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 prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → Zabezpečená připojení → Podle skupin**.
2. V levém podokně okna produktu System i Navigator klepněte 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 **Pravidlo filtrování zásad bude definováno v Pravidlech paketů**, musíte pak konfigurovat pravidla paketů VPN pomocí editoru pravidel paketů a potom je aktivovat.

Konfigurace ručních připojení

V ručním připojení musíte všechny vlastnosti VPN konfigurovat bez použití průvodců.

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.

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

Chcete-li definovat vlastnosti ručního připojení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → → Zabezpečená připojení**.
2. Klepněte pravým tlačítkem na **Všichni uživatelé** a vyberte **Nové ruční 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 **Ruční připojení - Připojení**. Vyberete-li však volbu **Pravidlo filtrování zásad bude definováno v Pravidlech paketů**, musíte pak konfigurovat pravidla filtrování zásad ručně a potom je aktivovat.

Související úlohy

“Konfigurace pravidel filtrování zásad” na stránce 52
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

Konfigurace dynamického připojení

Dynamické připojení dynamicky generuje a vyjednává klíče, které zabezpečují ochranu aktivního připojení pomocí protokolu IKE (Internet Key Exchange).

Postupujte podle průvodce novým dynamickým přiřazením klíče pro konfiguraci dynamického připojení a proveďte následující kroky:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → Zabezpečená připojení → Podle skupin**.
2. Klepněte pravým tlačítkem na určitou skupinu s dynamicky přiřazeným klíčem a vyberte **Nové připojení s dynamicky přiřazeným klíčem**.
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 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 System i Navigator, vytvořte také všechna další pravidla tímto způsobem. Pokud byla pravidla filtrování zásad vygenerována pomocí VPN, vytvořte také všechna další pravidla tímto způsobem.

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

- Konfigurace pravidla filtrování 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 pravidla filtrování napsaná speciálně pro povolení provozu IKE, je provoz IKE implicitně povolen.
- Konfigurace pravidel filtrování zásad

  Pravidlo filtrování 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 pravidla filtrování, 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 pravidel filtrování VPN. Chcete-li v rozhraní povolit jiný provoz než VPN, musíte přidat explicitní pravidla PERMIT.

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

Je velmi důležité, abyste pravidla filtrování konfigurovali řádně. Jinak mohou zablokovat veškerý příchozí i odchozí IP provoz v systému. Zahrnuje to i připojení k produktu System i Navigator, které používáte při konfiguraci pravidel filtrování.

Pokud pravidla filtrování nepovolují provoz systému System i, nemůže produkt System i Navigator komunikovat se systémem. Pokud dojde k této situaci, musíte se přihlásit do systému 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.

Související pojmy

“VPN a IP filtrování” na stránce 11
VPN a IP filtrování spolu úzce souvisejí. Většina připojení VPN vyžaduje pro řádné fungování pravidla filtrování. Toto téma uvádí, jaké filtry VPN vyžaduje, a seznamuje vás s koncepty filtrování souvisejícími s VPN.

Související úlohy

“Konfigurace zabezpečeného připojení VPN” na stránce 48
Až dokončíte konfiguraci zásad zabezpečení, musíte konfigurovat zabezpečené připojení.

"Konfigurace pravidla filtrování pre-IPSec"
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

"Konfigurace pravidel filtrování zásad" na stránce 52
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

"Definice rozhraní pro pravidla filtrování VPN" na stránce 53
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.

"Aktivace pravidel paketů VPN" na stránce 54
Před spuštěním vlastních připojení VPN musíte aktivovat pravidla paketů VPN.

Konfigurace pravidla filtrování pre-IPSec

Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování 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 pravidel filtrování, jedno pro příchozí a druhé pro odchozí provoz. Připojení pak může dynamicky vyjednávat klíče, které chrání připojení.

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 systém.
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 pravidla filtrování VPN. Doporučuje se vytvořit alespoň tři různé sady: jednu pro pravidla filtrování pre-IPSec, jednu pro pravidla filtrování zásad a jednu pro různá pravidla filtrování PERMIT a DENY. Jméno sady, která obsahuje pravidla filtrování 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 adresu IP lokálního klíčového serveru. Adresu IP 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 adresu IP vzdáleného klíčového serveru. Adresu IP 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 pravidel filtrování zásad . Určí se v něm, který IP provoz je připojením do VPN chráněn.

Související pojmy

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Související úlohy

"Konfigurace pravidel filtrování zásad"
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

Konfigurace pravidel filtrování zásad

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

Pravidlo filtrování 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 pravidlo filtrování 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 prostředí produktu System i Navigator rozbalte **Systém → 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 systém.
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 pravidla filtrování VPN. Doporučuje se vytvořit alespoň tři různé sady: jednu pro pravidla filtrování pre-IPSec, jednu pro pravidla filtrování zásad a jednu pro různá pravidla filtrování 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 adresu IP lokálního datového koncového systému. Můžete také zadat rozsah adres IP 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 adresu IP vzdáleného datového koncového systému. Můžete také zadat rozsah adres IP 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 pravidla filtrování 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 pravidla filtrování uplatněna.

Poznámka: Přidáte-li k nějakému rozhraní pravidla filtrování, 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.

Související pojmy

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Související úlohy

"Konfigurace ručních připojení" na stránce 49
V ručním připojení musíte všechny vlastnosti VPN konfigurovat bez použití průvodců.

"Konfigurace pravidla filtrování pre-IPSec" na stránce 51
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

"Definice rozhraní pro pravidla filtrování 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.

Definice rozhraní pro pravidla filtrování 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 pravidla filtrování VPN, postupujte takto:

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

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 systém.
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 ve vašem systému 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 pravidla filtrování, musíte ještě před spuštěním připojení VPN tato pravidla aktivovat.

Související pojmy

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Související úlohy

"Konfigurace pravidel filtrování zásad" na stránce 52
Tento úkol provádějte pouze tehdy, pokud jste zadali, že nechcete, aby pravidla filtrování zásad byla automaticky generována VPN.

"Aktivace pravidel paketů VPN"
Před spuštěním vlastních připojení VPN musíte aktivovat pravidla paketů VPN.

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 pravidel filtrování VPN zajistěte, aby žádné připojení, které je k němu přidružené, 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 pravidla filtrování zásad připojení VPN je nahradí.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 pravidel filtrování můžete spustit připojení VPN.

Související pojmy

"Konfigurace pravidel paketů VPN" na stránce 50
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.

Související úlohy

"Konfigurace zabezpečeného připojení VPN" na stránce 48
Až dokončíte konfiguraci zásad zabezpečení, musíte konfigurovat zabezpečené připojení.

"Definice rozhraní pro pravidla filtrování VPN" na stránce 53
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.

"Spuštění připojení VPN" na stránce 55
Až dokončíte tento úkol, budou lokálně iniciovaná připojení spuštěna.

Konfigurace funkce TFC (traffic flow confidentiality)

Je-li metoda pro práci s daty nakonfigurována pro režim Tunel, umožňuje funkce TFC (traffic flow confidentiality) zakrýt skutečnou délku datových paketů přenášených prostřednictvím připojení VPN.

Funkce TFC do odesílaných paketů přidá dodatečnou výplň a v náhodných intervalech odesílá fiktivní pakety s různými délkami. Tím zakrývá skutečnou délku paketů. Funkci TFC použijete pro dodatečné zabezpečení proti útočníkům, kteří se snaží podle délky datových paketů uhodnout typ odesílaných dat. Zapnutím funkce TFC získáte větší zabezpečení, avšak zároveň dojde ke snížení výkonu systému. Před a po zapnutí funkce TFC pro připojení VPN byste proto měli otestovat výkon svých systémů. Funkci TFC nevyjednává protokol IKE a uživatel by měl funkci TFC povolit pouze v případě, že ji oba systémy podporují.

Chcete-li povolit funkci TFC pro připojení VPN, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte server **> Síť → Zásady pro práci s IP → VPN → Zabezpečená připojení → Všechna připojení**.
2. Klepněte pravým tlačítkem na připojení, pro které chcete povolit funkci TFC, a vyberte **Vlastnosti**.
3. Na kartě **Obecné** vyberte volbu **V režimu Tunel použít funkci TFC**.

Konfigurace funkce ESN (extended sequence number)

Funkci ESN (extended sequence number) lze využít ke zvýšení rychlosti přenosu připojení VPN.

Používáte-li protokol AH nebo ESP a šifrovací algoritmus AES, pravděpodobně budete chtít zapnout funkci ESN. Funkce ESN umožňuje přenos velkých objemů dat velkou rychlostí, aniž by bylo třeba znovu nastavovat klíč. Připojení VPN používá přes IPSec 64bitová pořadová čísla místo 32bitových. 64bitová čísla prodlužují čas před opětovným nastavením klíče, čímž se zamezí vyčerpání pořadových čísel a minimalizuje využití systémových prostředků.

Chcete-li povolit funkci ESN pro připojení VPN, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN**.
2. Klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**.
3. Na kartě **Obecné** vyberte volbu **Použít ESN (Extended Sequence Number)**.

Spuštění připojení VPN

Až dokončíte tento úkol, budou lokálně iniciovaná připojení spuštěna.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP**.
2. Není-li server VPN spuštěn, klepněte pravým tlačítkem na **VPN (Virtual Private Networking)** a vyberte **Spustit**.
3. Přesvědčte se, že pravidla paketů jsou aktivována.
4. Rozbalte **VPN → 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**.

Související úlohy

"Aktivace pravidel paketů VPN" na stránce 54
Před spuštěním vlastních připojení VPN musíte aktivovat pravidla paketů VPN.

"Začínáme s odstraňováním problémů s VPN" na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

Správa VPN

Při provádění úloh správy VPN můžete používat rozhraní VPN v produktu System i Navigator. Mezi tyto úkoly patří zastavení připojení a zobrazení atributů připojení.

Při provádění úkolů správy používejte rozhraní VPN v produktu System i Navigator. Mezi tyto úkoly patří:

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.

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

Chcete-li nastavit předvolené hodnoty zabezpečení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → 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

Obnovou připojení v chybovém stavu vrátíte tato připojení do stavu Nečinný.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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

Až dokončíte tento úkol, můžete snáze určit, proč je připojení chybné.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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**.

Související úlohy

"Začínáme s odstraňováním problémů s VPN" na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

Prohlížení atributů aktivních připojení

Až dokončíte tento úkol, můžete zkontrolovat stav a ostatní atributy aktivních připojení.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → Zabezpečená připojení**.
2. Klepnutím na **Všechna připojení** zobrazíte seznam připojení v pravém podokně.
3. Klepnutím pravým tlačítkem na aktivní připojení nebo na připojení na vyžádání, které chcete prohlížet, a vyberte **Vlastnosti**.
4. Chcete-li prohlížet atributy tohoto připojení, přejděte na stranu **Aktuální atributy**.

V okně produktu System i 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 prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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 produktu System i 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.

Související pojmy

“Běžné chybové zprávy serveru Správce připojení VPN” na stránce 70
Při výskytu chyby zaznamená Správce připojení VPN do protokolu úlohy dvě zprávy.

Zobrazení trasování serveru VPN

Trasování serveru VPN 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.

Chcete-li prohlížet trasování serveru VPN, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → 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 stránce **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

Dodržujte tyto pokyny, chcete-li prohlížet protokoly úloh pro servery Správce klíčů VPN a Správce připojení VPN.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → 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

Až dokončíte tento úkol, budou zobrazeny atributy přidružení zabezpečení, které jsou přidruženy k aktivnímu připojení.

Chcete-li prohlížet atributy Přidružení zabezpečení (SA), které jsou přidruženy k aktivnímu připojení, postupujte takto:

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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 SA přidruženého k určitému připojení.

Zastavení připojení VPN

Až dokončíte tento úkol, budou aktivní připojení ukončena.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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

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.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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

Následující metody odstraňování problémů použijte k vyřešení některých základních problémů, s nimiž se můžete setkat při konfiguraci připojení k 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 pravidel filtrování. 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

Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

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 v systému 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 obvykle používá příkaz TRCTCPAPP, a získává tak výstup o trasování, který mu pomůže analyzovat problémy s připojením.

Související pojmy

"Požadavky na nastavení VPN" na stránce 41
Aby připojení k síti VPN řádně fungovalo na systémech a s klienty sítě, musíte splňovat minimální požadavky.

"Odstraňování problémů s VPN pomocí protokolů úloh VPN" na stránce 69
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.

"Odstraňování problémů s VPN pomocí trasování komunikace" na stránce 74
Systém IBM i5/OS 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.

Související úlohy

"Prohlížení informací o chybách" na stránce 56
Až dokončíte tento úkol, můžete snáze určit, proč je připojení chybné.

"Odstraňování problémů s VPN pomocí žurnálu QIPFILTER" na stránce 64
Toto téma uvádí informace o pravidlech filtrování VPN.

"Spuštění připojení VPN" na stránce 55
Až dokončíte tento úkol, budou lokálně iniciovaná připojení spuštěna.

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 adresu IP. 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 brány 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 pravidla filtrování 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 System i Navigator. Zajistěte, aby v pravidlech filtrování 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

S pomocí těchto informací zobrazte běžné chybové zprávy VPN a zjistěte jejich možná řešení.

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.

Chybová zpráva VPN: TCP5B28

Při pokusu o aktivaci pravidel filtrování v rozhraní vyvoláte zprávu TCP5B28 o narušení pořadí CONNECTION_DEFINITION

Příznak:

Při pokusu o aktivaci pravidel filtrování v rozhraní vyvoláte zprávu:

```
TCP5B28: Narušení pořadí CONNECTION_DEFINITION
```

Možné řešení:

pravidla filtrování, 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

Klepnutím pravým tlačítkem na objekt VPN a buď výběrem **Vlastnosti**, nebo výběrem **Vymazat** vyvoláte zprávu **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:

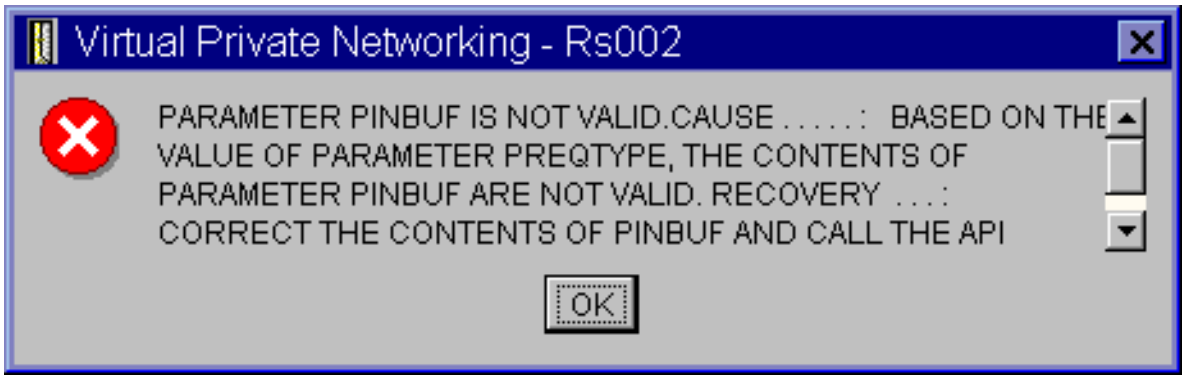
- Možná byl objekt vymazán nebo přejmenován a okno VPN (Virtual Private Networking) ještě nebylo obnoveno. V důsledku toho je objekt v okně ještě zobrazen. Chcete-li toto tvrzení ověřit, vyberte v menu **Zobrazení** příkaz **Obnovit**. Je-li objekt stále v okně VPN (Virtual Private Networking) zobrazen, pokračujte další položkou na tomto seznamu.
- Při konfiguraci vlastností objektu mohlo dojít k chybě v komunikaci mezi serverem VPN a vaším systémem. Mnohé objekty, které jsou zobrazeny v okně VPN, 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

Při pokusu o spuštění připojení vyvoláte zprávu **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...

Vyberete-li **Vlastnosti** u připojení s dynamicky přiřazeným klíčem, vyvoláte chybu, která říká, že server nemohl najít zadaný vzdálený klíčový server.

Příznak:

Vyberete-li **Vlastnosti** u připojení s dynamicky přiřazeným klíčem, zobrazí se zpráva podobná této:

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

Klepnutím na tlačítko **OK** na listu vlastností pro skupinu s dynamicky přiřazeným klíčem nebo pro ruční připojení vyvoláte zprávu, která říká, že systém nemůže objekt aktualizovat.

Příznak:

Klepnutím na tlačítko **OK** na listu vlastností pro skupinu s dynamicky přiřazeným klíčem nebo pro ruční 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...

Dostanete zprávu, která říká, že systém nemůže zakódovat vaše klíče, protože QRETSVRSEC musí mít hodnotu 1.

Příznak:

Zobrazí se následující 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 ručním 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**.

Související pojmy

“Chyba VPN: Všechny klíče jsou prázdné” na stránce 63

Všechny předem nasdílené klíče pro připojení jsou při prohlížení vlastností ručního připojení prázdné.

Chybová zpráva VPN: CPF9821

Při pokusu o rozbalení nebo otevření zásobníku zásad pro práci s IP v produktu System i Navigator se zobrazí zpráva CPF9821- Nemáte oprávnění k programu QTFRPRS v knihovně QSYS.

Příznak:

Při pokusu o rozbalení nebo otevření zásobníku zásad pro práci s IP v produktu System i Navigator se zobrazí 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 System i Navigator, musíte mít oprávnění *IOSYSCFG.

Chyba VPN: Všechny klíče jsou prázdné

Všechny předem nasdílené klíče pro připojení jsou při prohlížení vlastností ručního připojení prázdné.

Příznak:

Všechny předem nasdílené klíče a klíče algoritmů pro ruční 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.

Související pojmy

"Chybová zpráva VPN: Nelze zakódovat klíč..." na stránce 62

Dostanete zprávu, která říká, že systém nemůže zakódovat vaše klíče, protože QRETSVRSEC musí mít hodnotu 1.

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

Při prvním použití rozhraní pravidel paketů v systému System i Navigator se zobrazí přihlášení do jiného než aktuálního 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 System i Access for Windows získat příslušné převodní tabulky pro kódování Unicode. Tato situace nastane pouze jednou.

Chyba VPN: Prázdný stav připojení v okně System i Navigator

Ve sloupci **Stav** v okně produktu System i Navigator chybí hodnota pro toto připojení.

Příznak:

Ve sloupci **Stav** v okně produktu System i Navigator chybí hodnota pro toto připojení.

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

Po ukončení připojení indikuje okno produktu System i Navigator, že připojení je stále aktivní.

Příznak:

Po ukončení připojení indikuje okno produktu System i Navigator, že připojení je stále aktivní.

Možné řešení:

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

Chyba VPN: 3DES není pro šifrování k dispozici

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

Příznak:

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

Možné řešení:

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

klíčů. Produkty Cryptographic Access Provider (5722-AC2) a (5722-AC3) již nejsou požadovány pro povolení šifrování dat na systémech, kde je spuštěn OS i5/OS V5R4 nebo vyšší.

Chyba VPN: V okně produktu System i Navigator se zobrazily neočekávané sloupce

V okně produktu System i Navigator jste nastavili sloupce, které chcete pro připojení VPN zobrazit. Když se na něj podíváte později, jsou zobrazeny jiné sloupce.

Příznak:

V okně produktu System i Navigator jste nastavili sloupce, které chcete pro připojení VPN zobrazit. Když se na něj 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 pravidla filtrování nelze deaktivovat

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

Příznak:

Při pokusu o deaktivaci aktuální množiny pravidel filtrování 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 pravidla filtrování deaktivovat.

Chyba VPN: Změna skupiny s 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.

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 přidružit 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

Toto téma uvádí informace o pravidlech filtrování VPN.

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

Související úlohy

"Začínáme s odstraňováním problémů s VPN" na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

Aktivace žurnálu QIPFILTER

Chcete-li aktivovat žurnál QIPFILTER, použijte editor pravidel paketů v produktu System i Navigator.

Funkci protokolování musíte aktivovat pro každé jednotlivé pravidlo filtrování. 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 pravidlo filtrování:

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

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

Použití žurnálu QIPFILTER

Operační systém i5/OS 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 pravidla filtrování, ve kterých je volba žurnálování nastavena na hodnotu FULL. Pokud jste například nastavili pouze pravidla filtrování 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 pravidlo filtrování, 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 pravidla filtrování. Po otestování sad filtrů zredukujte žurnálování na únosnou míru.

Související pojmy

"Pole žurnálu QIPFILTER"
Prohlédněte následující tabulku, která popisuje pole ve výstupním souboru QIPFILTER.

Pole žurnálu QIPFILTER

Prohlédněte následující tabulku, která 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	Časové označení 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

Jméno pole	Délka pole	Numerické	Popis	Poznámka
TFPROT	4	N	Transportní protokol	1 je ICMP 6 je TCP 17 je UDP 50 je ESP 51 je AH
TFSRCA	15	N	Zdrojová adresa IP	
TFSRCP	5	N	Zdrojový port	Přebytečný bajt, pokud TFPROT= 1 (ICMP)
TFDSTA	15	N	Cílová adresa IP	
TFDSTP	5	N	Cílový port	Přebytečný bajt, pokud TFPROT= 1 (ICMP)
TFTEXT	76	N	Další text	Obsahuje popis, pokud TFREVT= L* nebo U*

Související úlohy

"Použití žurnálu QIPFILTER" na stránce 65
Operační systém i5/OS automaticky vytvoří žurnál, když poprvé aktivujete filtr IP paketu.

Odstraňování problémů s VPN pomocí žurnálu QVPN

Toto téma uvádí informace o IP provozu a připojeních.

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 QVPN

Chcete-li aktivovat žurnál VPN, použijte rozhraní VPN v produktu System i Navigator.

Neexistuje funkce, která aktivuje protokolování pro všechna připojení VPN. Proto musíte aktivovat funkci protokolování pro každou jednotlivou skupinu s dynamicky přiřazeným klíčem nebo ruční připojení.

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

1. V prostředí produktu System i Navigator rozbalte **Systém → Síť → Zásady pro práci s IP → VPN → 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 ruční připojení rozbalte **Všechna připojení** a potom klepněte pravým tlačítkem na ruční 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 přidružený s tomuto připojení. Při každém vyvolání pravidla filtrování 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 k této skupině nejsou přidružena žádná aktivní připojení.

Použití žurnálu QVPN

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.

Související pojmy

"Pole žurnálu QVPN"
Prohlédněte následující tabulku, která popisuje pole ve výstupním souboru QVPN.

Pole žurnálu QVPN

Prohlédněte následující tabulku, která 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	Časové označení 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	

Jméno pole	Délka pole	Numerické	Popis	Poznámka
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	
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	Kód chyby	

Související úlohy

“Použití žurnálu QVPN” na stránce 68
Chcete-li prohlížet podrobnosti specifické pro záznam v žurnálu VPN, můžete záznamy žurnálu zobrazit na obrazovce nebo můžete použít výstupní soubor.

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 modely System i. Když selže spuštění dynamického připojení, je užitečné vědět, co se děje ve vzdáleném systému.

V subsystému QSYSWRK jsou spuštěny tyto úlohy VPN: QTOVMAN a QTOKVPNIKE. V produktu System i 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.

Související úlohy

“Začínáme s odstraňováním problémů s VPN” na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

Běžné chybové zprávy serveru Správce připojení VPN

Při výskytu chyby zaznamená Správce připojení VPN do protokolu úlohy dvě zprávy.

První zpráva poskytuje podrobnosti týkající se chyby. Informace o těchto chybách můžete v prostředí produktu System i 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.	Připojení VPN nelze spustit v důsledku jedné z příčin s tímto kódem: *0* - Předchozí zpráva v protokolu úlohy se stejným jménem připojení 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 System i Navigator. Připojení, která nelze spustit, budou v chybovém stavu.

Chybové zprávy serveru Správce připojení VPN

Zpráva	Příčina	Obnova
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 kódů příčiny: *0* - Předchozí zpráva v protokolu úlohy se stejným jménem připojení 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 System i Navigator. Připojení, která nelze spustit, budou v chybovém stavu.
TCP8604 Spuštění připojení [*jméno připojení*] do VPN selhalo.	Spuštění připojení VPN selhalo z důvodů popsaných jedním z těchto kódů příčiny: *1* - Jméno vzdáleného hostitelského systému nelze převést na adresu IP. *2* - Jméno lokálního hostitelského systému nelze převést na adresu IP. *3* - Pravidlo filtrování zásad VPN přidružené k tomuto připojení do VPN není zavedeno. *4* - Hodnota klíče zadaná uživatelem není platná pro přidružený 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 System i Navigator. Zajistěte, aby skupina dynamických klíčů přidružená k tomuto připojení 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.

Chybové zprávy serveru Správce připojení VPN

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 kódů příčiny: *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 System i Navigator. Zajistěte, aby skupina dynamických klíčů přidružená k tomuto připojení 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 kódů příčiny: *1* - Adresa, na kterou se má použít NAT, není jednotlivá adresa IP. *2* - Všechny dostupné adresy jsou již použity.	1. Další zprávy najdete v protokolech úloh. 2. Opravte chyby a zopakujte požadavek. 3. Zkontrolujte nebo opravte zásadu VPN pomocí produktu System i Navigator. Zajistěte, aby skupina dynamických klíčů přidružená k tomuto připojení 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.
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.

Chybové zprávy serveru Správce připojení VPN

Zpráva	Příčina	Obnova
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 přidruženou k tomuto připojení VPN pomocí produktu System i 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 System i Navigator. Změňte zásadu stávajícího připojení, pokud jsou obě připojení vyžadována. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8624 Připojení VPN je mimo rozsah přidruženého pravidla filtrování zásad.	Toto připojení VPN nelze aktivovat, protože datové koncové systémy jsou mimo rozsah definovaného pravidla filtrování 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 System i Navigator. Jsou-li vybrány volby **Podmnožina filtrů zásad** nebo **Přizpůsobení filtru zásad**, zkontrolujte datové koncové systémy tohoto připojení. Měly by vyhovovat aktivnímu pravidlu filtrování, které má jméno akce IPSEC a jméno připojení VPN přidružené k tomuto připojení. Chcete-li toto připojení aktivovat, změňte zásadu stávajícího připojení nebo pravidlo filtrování. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8625 Selhala kontrola připojení VPN pomocí algoritmu protokolu ESP.	Toto připojení VPN nelze aktivovat, protože tajný klíč přidružený k připojení je nedostatečný.	1. Další zprávy týkající se tohoto připojení najdete v protokolech úloh. 2. Chcete-li zobrazit zásadu přidruženou k tomuto připojení a zadat jiný tajný klíč, použijte produkt System i Navigator. 3. Opravte všechny chyby a zopakujte požadavek.

Chybové zprávy serveru Správce připojení VPN

Zpráva	Příčina	Obnova
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 System i Navigator. Jsou-li vybrány volby **Podmnožina filtrů zásad** nebo **Přizpůsobení filtru zásad**, zkontrolujte datové koncové systémy tohoto připojení. Měly by vyhovovat aktivnímu pravidlu filtrování, které má jméno akce IPSEC a jméno připojení VPN přidružené k tomuto připojení. Chcete-li toto připojení aktivovat, změňte zásadu stávajícího připojení nebo pravidlo filtrování. 3. Opravte všechny chyby a zopakujte požadavek.
TCP8628 Pravidlo filtrování zásad není zavedeno.	Pravidlo filtrování 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 System i Navigator. Zkontrolujte pravidlo filtrování 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 System i Navigator. 3. Opravte všechny chyby a zopakujte požadavek.
TCP862A Připojení profilu PPP se nezdařilo.	Toto připojení VPN bylo přidruženo k profilu 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 přidružené k profilu PPP. 3. Opravte všechny chyby a zopakujte požadavek.

Související úlohy

“Prohlížení atributů aktivních připojení” na stránce 56
Až dokončíte tento úkol, můžete zkontrolovat stav a ostatní atributy aktivních připojení.

Odstraňování problémů s VPN pomocí trasování komunikace

Systém IBM i5/OS 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 adresy IP, 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 adresy IP, 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 adresu IP, 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 úlohy

“Začínáme s odstraňováním problémů s VPN” na stránce 58
Proveďte tuto úlohu, abyste se naučili různé metody určování problémů s VPN na systému.

Související informace pro VPN

Příručky IBM Redbooks a webové stránky obsahují informace, které souvisejí s množinou témat týkajících se sítě VPN (Virtual private networking). Libovolný z těchto souborů PDF můžete zobrazit nebo vytisknout.

IBM Redbooks

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

Webové stránky

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

- TCP/IP for i5/OS: RFC Documents 

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabídnout 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 Česká republika, spol. s r.o.
North Castle Drive
Armonk, NY 10504-1785
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 106-0032, 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" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností 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.

Jakékoliv 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 jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv 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 Česká republika, spol. s r.o.
Software Interoperability Coordinator, Department YBWA
Česká republika

Rochester, MN 55901
U.S.A.

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

Zde popsaný licencovaný program a všechny licencované materiály, které jsou pro něj k dispozici, poskytuje IBM na základě smlouvy IBM Customer Agreement, Mezinárodní licenční smlouvy IBM na programy, smlouvy IBM License Agreement for Machine Code, nebo jiné ekvivalentní smlouvy mezi námi.

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 od jiných dodavatelů, musí být adresovány příslušným dodavatelům.

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

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.

COPYRIGHT

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyce, které demonstrují techniku programování na různých operačních systémech. Tyto vzorové programy můžete bez závazků vůči IBM jakýmkoliv způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly přísně testovány za všech podmínek. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Každá kopie nebo oblast těchto vzorových programů nebo odvozených prací musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno Vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů IBM Corp. © Copyright IBM Corp. __zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Tato publikace o síti VPN je určena pro programovací rozhraní, které umožňuje zákazníkům psát programy za účelem získání služeb operačního systému IBM i5/OS.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

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

Adobe, logo Adobe, PostScript a logo PostScript jsou registrované ochranné známky nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech, případně 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.

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

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

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 nebo jakékoliv 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 jeho 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. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.