System i

Sigurnosno
Virtualno privatno umrežavanje

Verzija 6 Izdanje 1

System i

Sigurnosno
Virtualno privatno umrežavanje

Verzija 6 Izdanje 1

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 77.

Ovo izdanje se odnosi na verziju 6, izdanje 1, preinaku 0 za IBM i5/OS (broj proizvoda 5761-SS1) i sva sljedeća izdanja i preinake dok se drugačije ne označi u novim izdanjima. Ova verzija ne radi na svim računalima sa smanjenim skupom instrukcija (RISC), niti ne radi na CISC modelima.

Sadržaj

Virtualno privatno umrežavanje

Virtualna privatna mreža (VPN) dozvoljava vašem poduzeću da sigurno proširi svoj privatni intranet preko postojećeg sistema javne mreže, kao što je Internet. S VPN-om vaše poduzeće može kontrolirati mrežni promet i ujedno ponuditi važna svojstva sigurnosti, kao što su provjera autentičnosti i privatnost podataka.

VPN je opcijski instalirana komponenta System i Navigator, grafičkog korisničkog sučelja (GUI) za i5/OS. Ona vam dozvoljava da kreirate sigurnu stazu od kraja do kraja između bilo koje kombinacije hosta i prilaza. VPN koristi metode provjere autentičnosti, algoritme šifriranja i ostale preventivne mjere kako bi se osiguralo da podaci koji se šalju između dvije krajnje točke pri vezi ostanu sigurni.

VPN se izvodi na sloju mreže TCP/IP stack modela slojevitih veza. Specifično, VPN koristi otvoreni sistem IP sigurnosne arhitekture (IPSec). IPSec omogućuje osnovne funkcije sigurnosti za Internet, a isto tako nabavlja fleksibilne građevne blokove iz kojih zatim možete kreirati jake, sigurne virtualne privatne mreže.

VPN također podržava Sloj 2 tunelski protokol (L2TP) VPN rješenja. L2TP veze, također zvane virtualne linije, omogućuju isplativ pristup udaljenim korisnicima time što dozvoljavaju poslužitelju korporativne mreže da upravlja IP adresama dodijeljenim njegovim udaljenim korisnicima. Nadalje, L2TP veze omogućuju siguran pristup vašem sistemu ili mreži kada ih štitite koristeći IPSec.

Vrlo je važno da razumijete efekt koji će VPN imati na cijeloj vašoj mreži. Ispravno planiranje i implementacija su važni za vaš uspjeh. Pregledajte ova poglavlja za osiguranje da znate kako VPN-ovi rade i kako bi ih koristili:

Što je novo za V6R1

Pročitajte o novim ili značajno promijenjenim informacijama za zbirku poglavlja Virtualnog privatnog umrežavanja.

Nova funkcija: IP verzija 6

Sada možete koristiti IP verziju 6 da kreirate VPN sa sljedećim tipovima veze: host-to-host, host-to-gateway, i gateway-to-gateway. VPN veze podržavaju IP verziju 6 za adresu, raspon, podmrežu i ime hosta. Svi VPN čarobnjaci su ažurirani za prihvaćanje nove IP verzije 6 ID tipova.

- Internet Protocol verzija 6

Kako vidjeti što ima novo ili je promijenjeno

Da vam pomogne vidjeti učinjene tehničke promjene, ove informacije koriste:

- Sliku » da označi gdje nova ili promijenjena informacija počinje.
- Sliku « da označi gdje nova ili promijenjena informacija završava.

Da nađete druge informacije o tome što je novo ili promijenjeno u ovom izdanju pogledajte Memorandum korisnicima.

PDF datoteka za Virtualnu privatnu mrežu

Možete pogledati i ispisati PDF datoteku s ovim informacijama.

Da pogledate ili preuzmete PDF verziju ovog dokumenta, izaberite Virtualna privatna mreža (VPN)  (oko 1100KB).

Spremanje PDF datoteka

Da spremite PDF na vašu radnu stanicu za gledanje ili ispis:

1. Desno kliknite PDF vezu u svom pretražitelju.
2. Kliknite **Save Target As** ako koristite Internet Explorer. Kliknite **Save Link As** ako koristite Netscape Communicator.
3. Otiđite do direktorija u koji želite spremiti PDF.
4. Kliknite **Save**.

Preuzimanje Adobe Acrobat Readera

Trebate Adobe Acrobat Reader za gledanje ili ispis ovih PDF-ova. Možete preuzeti kopiju s Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html) .

VPN koncepti

Važno je da imate bar osnovno znanje o standardnim VPN tehnologijama prije implementacije VPN veze.

Virtualno privatno umrežavanje (VPN) koristi nekoliko važnih TCP/IP protokola da zaštiti promet podataka. Da biste bolje razumjeli kako radi VPN veza, upoznajte se s tim protokolima i konceptima i kako ih VPN koristi:

IP Sigurnosni protokoli

IP Sigurnost (IPSec) osigurava stabilnu, dugotrajnu bazu za osiguravanje sigurnosti mrežnog sloja.

IPSec podržava sve kriptografske algoritme koji su danas u upotrebi i može smjestiti novije, moćnije algoritme čim postanu dostupni. IPSec protokoli adresiraju ova glavna pitanja sigurnosti:

Provjera autentičnosti porijekla podataka
Provjerava da svaki datogram potiče od navedenog odašiljača.

Integritet podataka
Provjerava da sadržaji datograma nisu promijenjeni u prijenosu, bilo namjerno ili zbog slučajnih pogrešaka.

Povjerljivost podataka
Skriva sadržaj poruke, najčešće korištenjem šifriranja.

Zaštita replaya
Osigurava da napadač ne može presresti datogram i izvoditi ga u nekom naknadnom trenutku

Automatsko upravljanje kriptografskih ključeva i sigurnosne asocijacije
Osigurava da se vaša VPN politika može koristiti preko cijele proširene mreže s malo ili bez ručne konfiguracije.

VPN koristi dva IPSec protokola da zaštiti podatke za vrijeme protoka kroz VPN: Zaglavlje za provjeru autentičnosti (AH) i Sažimanje tereta sigurnosti (ESP). Drugi dio omogućenja IPSec je protokol Internet razmjene ključeva (IKE) ili upravljanje ključem. Dok IPSec šifrira vaše podatke, IKE podržava automatizirane pregovore sigurnosnih asocijacija (SA) i automatizirano generiranje i osvježavanje kriptografskih ključeva.

Bilješka: Neke VPN konfiguracije mogu biti sigurnosno ranjive, ovisno o konfiguraciji IPSec-a. Ranjivost utječe na konfiguracije gdje je IPSec konfiguriran za korištenje Encapsulating Security Payload (ESP) u tunel načinu s povjerljivosti (šifriranje), ali bez zaštite integriteta (provjere autentičnosti) ili Zaglavlja provjere autentičnosti (AH). Default konfiguracija kad je ESP izabran uvijek uključuje algoritam provjere autentičnosti koja osigurava zaštitu integriteta. Zato, osim ako je uklonjen algoritam provjere autentičnosti u pretvorbi ESP, VPN konfiguracije će biti zaštićene od ovog propusta. IBM VPN konfiguracija Univerzalne veze ne utječe na ovaj propust.

Slijedite ove korake kako biste provjerili da li na vaš sistem utječe sigurnosna ranjivost:

1. U System i Navigator, proširite **sistem → Mrežu → IP politike → Virtualno privatno umrežavanje → IP Sigurnosne politike → Politike podataka** .
2. Desno kliknite na politiku podataka koju želite provjeriti i izaberite **Svojstva**.
3. Kliknite na karticu **Prijedlozi**.
4. Izaberite bilo koji prijedlog zaštite podataka koje koriste ESP protokol i kliknite **Uredi**.
5. Kliknite na karticu **Pretvaranje**.
6. Izaberite bilo koje pretvaranje s popisa koji koristi ESP protokol i kliknite **Uredi**.
7. Provjerite da Algoritam provjere autentičnosti ima bilo koju vrijednost osim **Ni jedan**.

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira IPSec u Zahtjevu za komentarima (RFC) 2401, *Sigurnosna arhitektura za Internet protokol*. Pregledajte ovaj RFC na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Glavni IPSec protokoli navedeni su na donjem popisu:

Srodni koncepti

“Upravljanje ključevima” na stranici 6
Dinamički VPN daje dodatnu sigurnost za vaše komunikacije korištenjem protokola Internet razmjena ključa (IKE) za upravljanje ključem. IKE dozvoljava VPN poslužiteljima na svakom kraju veze da pregovaraju nove ključeve u određenim intervalima.

Srodne informacije

http://www.rfc-editor.org

Zaglavlje za provjeru autentičnosti

Protokol Zaglavlje za provjeru autentičnosti (AH) omogućava provjeru autentičnosti porijekla podataka, integriteta podataka i zaštitu od ponovljenog izvođenja. Međutim, AH ne omogućava povjerljivost podataka, što znači da se svi vaši podaci šalju u jasnom obliku.

AH osigurava integritet podataka pomoću kontrolne sume koju generira kod za provjeru autentičnosti poruke, kao na primjer MD5. Da biste osigurali provjeru autentičnosti porijekla podataka, AH uključuje tajni dijeljeni ključ u algoritmu koji se koristi za provjeru autentičnosti. Da osigura zaštitu od ponovljenog izvođenja, AH koristi polje za redni broj unutar AH zaglavlja. Ovdje nije važno to da su ove tri različite funkcije često zajedno sjedinjene i na njih se upućuje kao na provjeru autentičnosti. U najjednostavnijim uvjetima AH osigurava da vaši podaci nisu loše radili s en smjerom do svog konačnog odredišta.

Iako AH radi provjeru autentičnosti IP datograma u što je moguće većoj mjeri, primalac nije u mogućnosti predvidjeti vrijednosti određenih polja u IP zaglavlju. AH ne štiti ova polja, poznata kao promjenjiva polja. Međutim, AH uvijek štiti teret IP paketa.

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira AH u Zahtjevu za komentar (RFC) 2402, *Zaglavlje za IP provjeru autentičnosti*. Pregledajte ovaj RFC na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Načini upotrebe AH

AH možete primijeniti na dva načina: transportni način ili tunelski način. U transportnom načinu, IP zaglavlje datograma je krajnje vanjsko IP zaglavlje, slijedi ga AH zaglavlje i zatim teret datograma. AH provjerava autentičnost cijelog datograma, osim promjenjivih polja. Međutim, informacije sadržane u datogramu transportirane su u jasnom obliku i stoga su podložne ’prisluškivanju’. Transportni način zahtijeva manje opterećenje pri obradi od tunelskog načina, ali ne omogućuje toliku sigurnost.

Tunelski način kreira novo IP zaglavlje i koristi ga kao krajnje vanjsko IP zaglavlje datograma. AH zaglavlje slijedi novo IP zaglavlje. Originalni datogram (oboje, IP zaglavlje i originalni teret) dolazi zadnji. AH radi provjeru autentičnosti cijelog datograma, što znači da odgovarajući sistem može otkriti da li je datogram promijenjen za vrijeme prolaska.

Kada je bilo koji kraj sigurnosne asocijacije prilaz, koristite tunelski način. U tunelskom načinu, adrese izvora i odredišta u krajnjem vanjskom IP zaglavlju ne trebaju biti iste kao one u originalnom IP zaglavlju. Na primjer, dva sigurnosna prilaza mogu djelovati na AH tunel da provjeri autentičnost cijelog prometa između mreža koje zajedno povezuju. Zapravo, ovo je vrlo tipična konfiguracija.

Glavna prednost korištenja tunelskog načina je to što tunelski način u potpunosti štiti sažeti IP datogram. Dodatno, tunelski način čini mogućim korištenje privatnih adresa.

Zašto AH?

U mnogim slučajevima vaši podaci zahtijevaju samo provjeru autentičnosti. Dok protokol Encapsulating Security Payload (ESP) može izvesti provjeru autentičnosti, AH ne utječe na sistemske performanse kao što radi ESP. Druga prednost korištenja AH je to da AH provjerava autentičnost cijelog datograma. Međutim, ESP ne provjerava autentičnost vodećeg IP zaglavlja ili bilo koje druge informacije koje dolaze prije ESP zaglavlja.

Dodatno, ESP zahtijeva snažne kriptografske algoritme kako bi se mogao koristiti. U nekim regijama ograničena je stroga kriptografija, dok AH nije reguliran i može se slobodno koristiti svuda.

Korištenje ESN s AH

Ako koristite AH protokol možete omogućiti Proširen redni broj (ESN). ESN omogućava prijenos velikog obujma podataka pri visokim brzinama bez ponovnog kriptiranja. VPN veza koristi 64-bit redne brojeve umjesto 32-bit brojeva preko IPSec. Korištenje 64-bit rednih brojeva omogućava više vremena prije ponovnog kriptiranja, što sprečava iscrpljenje rednih brojeva i smanjuje korištenje sistemskih resursa.

Koje algoritme koristi AH za zaštitu informacija?

AH koristi algoritme kao što su **kodovi provjere autentičnosti raspršene poruke (HMAC).** Specifično, VPN koristi ili HMAC-MD5 ili HMAC-SHA. Oba algoritma, MD5 i SHA, uzimaju ulazne podatke promjenjive dužine i tajni ključ da bi proizveli izlazne podatke fiksne dužine (poznate kao vrijednost raspršenja). Ako se raspršenja dvije poruke podudaraju, velika je vjerojatnost da su te poruke jednake. Oba algoritma, MD5 i SHA, kao izlaz imaju kodiranu dužinu poruke, ali SHA protokol se smatra sigurniji zato što proizvodi veća raspršenja.

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira HMAC-MD5 u Zahtjevu za komentarima (RFC) 2085, *HMAC-MD5 IP provjera autentičnosti sa sprečavanjem ponavljanja izvođenja*. Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira HMAC-SHA u Zahtjevu za komentarima (RFC) 2404, *Upotreba HMAC-SHA-1-96 unutar ESP i AH*. Pregledajte ove RFC-eve na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Srodni koncepti

“Sažimanje tereta sigurnosti”
Protokol Sažimanje tereta sigurnosti (ESP) omogućuje povjerljivost podataka, a također opcijski omogućuje provjeru autentičnosti porijekla podataka, provjeru integriteta podataka i zaštitu od ponovljenog izvođenja.

Srodne informacije

http://www.rfc-editor.org

Sažimanje tereta sigurnosti

Protokol Sažimanje tereta sigurnosti (ESP) omogućuje povjerljivost podataka, a također opcijski omogućuje provjeru autentičnosti porijekla podataka, provjeru integriteta podataka i zaštitu od ponovljenog izvođenja.

Razlika između ESP i protokola Zaglavlja provjere autentičnosti (AH) je da ESP osigurava šifriranje, dok oba protokola osiguravaju provjeru autentičnosti, provjeru integriteta i replay zaštitu. S ESP protokolom, oba sistema za komunikaciju koriste dijeljeni ključ za šifriranje i dešifriranje podataka koje izmjenjuju.

Ako odlučite koristiti oboje, šifriranje i provjeru autentičnosti, tada sistem koji odgovara najprije radi provjeru autentičnosti paketa, a zatim, ako prvi korak uspije, sistem nastavlja s dešifriranjem. Ovaj tip konfiguracije smanjuje opterećenje kod obrade i također smanjuje vašu ranjivost na napade tipa 'odbijanje usluge'.

Dva načina korištenja ESP-a

ESP možete primijeniti na dva načina: transportni način ili tunelski način. U transportnom načinu, ESP zaglavlje slijedi IP zaglavlje originalnog IP datograma. Ako datogram već ima IPSec zaglavlje, tada ESP zaglavlje ide prije njega. ESP ostatak i opcijski podaci za provjeru autentičnosti slijede teret.

Transportni način ne autentificira ili šifrira IP zaglavlje, što može otkriti vaše adresne informacije potencijalnom napadaču dok se datogrami prenose. Transportni način zahtijeva manje opterećenje pri obradi od tunelskog načina, ali ne omogućuje toliku sigurnost. U većini slučajeva, hostovi koriste ESP u transportnom načinu.

Tunelski način kreira novo IP zaglavlje i koristi ga kao krajnje vanjsko IP zaglavlje datograma, koje slijedi ESP zaglavlje i zatim originalni datogram (oboje, IP zaglavlje i originalni teret). ESP ostatak i opcijski podaci za provjeru autentičnosti pridodani su teretu. Kada koristite oboje, šifriranje i provjeru autentičnosti, ESP u potpunosti štiti originalni datogram, jer on sada čini podatke tereta za novi ESP paket. Međutim, ESP ne štiti nova IP zaglavlja. Prilazi moraju koristiti ESP u tunelskom načinu.

Koje algoritme koristi ESP za zaštitu informacija?

ESP koristi simetrični ključ koji obje strane uključene u komunikaciju koriste za šifriranje podataka koje razmjenjuju. Odašiljač i primalac se moraju složiti oko ključa prije nego se među njima izvede sigurna komunikacija. Za šifriranje VPN koristi Standard šifriranja podataka (DES), trostruki-DES (3DES), RC5, RC4 ili Standard naprednog šifriranja (AES).

Ako za šifriranje koristite AES algoritam, možete omogućiti Prošireni redni broj (ESN). ESN omogućava prijenos velikog obujma podataka pri visokim brzinama. VPN veza koristi 64-bit redne brojeve umjesto 32-bit brojeva preko IPSec. Korištenje 64-bit rednih brojeva omogućava više vremena prije ponovnog kriptiranja, što sprečava iscrpljenje rednih brojeva i smanjuje korištenje sistemskih resursa.

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira DES u Zahtjevu za komentarima (RFC) 1829, *ESP DES-CBC pretvorba*. IETF formalno definira 3DES u RFC 1851, *ESP trostruka DES pretvorba*. Pregledajte ove RFC-eve na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

ESP koristi HMAC-MD5 i HMAC-SHA algoritme da omogući funkcije za provjeru autentičnosti. Oba algoritma, MD5 i SHA, uzimaju ulazne podatke promjenjive dužine i tajni ključ da bi proizveli izlazne podatke fiksne dužine (poznate kao vrijednost raspršenja). Ako se raspršenja dvije poruke podudaraju, velika je vjerojatnost da su te poruke jednake. Oba algoritma, MD5 i SHA, kao izlaz imaju kodiranu dužinu poruke, ali SHA protokol se smatra sigurniji zato što proizvodi veća raspršenja.

IETF formalno definira HMAC-MD5 u RFC 2085, *HMAC-MD5 IP Provjeru autentičnosti sa sprečavanjem odgovora*. IETF formalno definira HMAC-SHA u RFC 2404, *Upotreba HMAC-SHA-1-96 unutar ESP i AH*. Pregledajte ove RFC-eve na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Srodni koncepti

"Zaglavlje za provjeru autentičnosti" na stranici 3
Protokol Zaglavlje za provjeru autentičnosti (AH) omogućava provjeru autentičnosti porijekla podataka, integriteta podataka i zaštitu od ponovljenog izvođenja. Međutim, AH ne omogućava povjerljivost podataka, što znači da se svi vaši podaci šalju u jasnom obliku.

Srodne informacije

http://www.rfc-editor.org

AH i ESP kombinirano

VPN vam dozvoljava kombiniranje AH i ESP protokola za host-host povezivanja u načinu prijenosa.

Kombiniranje ovih protokola štiti cijeli IP datogram. Premda kombiniranje dvaju protokola nudi više sigurnosti, obrada uključenog opterećenja bi mogla nadjačati korist.

Upravljanje ključevima

Dinamički VPN daje dodatnu sigurnost za vaše komunikacije korištenjem protokola Internet razmjena ključa (IKE) za upravljanje ključem. IKE dozvoljava VPN poslužiteljima na svakom kraju veze da pregovaraju nove ključeve u određenim intervalima.

Sa svakim uspješnim pregovaranjem, VPN poslužitelji obnavljaju ključeve koji štite vezu, a time čine puno težim za mogućeg napadača da uhvati informacije iz veze. Uz to, ako koristite savršenu prethodnu tajnovitost, napadači ne mogu izvesti buduće ključeve na bazi prošlih informacija o ključevima.

VPN upravitelj ključa je IBM-ova implementacija protokola Internet Key Exchange (IKE). Upravitelj ključeva podržava automatsko pregovaranje sigurnosnih asocijacija (SA), kao i automatsko generiranje i osvježavanje kriptografskih ključeva.

Sigurnosna asocijacija (SA) sadrži informacije koje su potrebne za korištenje IPSec protokola. Na primjer, SA identificira tipove algoritama, dužine ključeva i njihovo vrijeme života, sudionike koji sudjeluju i načine sažimanja.

Kriptografski ključevi, kao što samo ime govori, zaključavaju ili štite vaše informacije sve dok ne dosegnu konačno odredište.

Bilješka: Sigurno generiranje ključeva najbitniji je faktor u uspostavljanju sigurne i privatne veze. Ako su vaši ključevi ugroženi, tada vaša nastojanja provjere autentičnosti i šifriranja, bez obzira koliko jaka, postaju beznačajna.

Faze upravljanja ključem

Upravitelj VPN ključa koristi dvije različite faze u svojoj primjeni.

Faza 1 Faza 1 uspostavlja glavnu tajnu iz koje se izvode svi naredni kriptografski ključevi u svrhu zaštite prometa podataka korisnika. Ovo je točno, čak i ako još ne postoji sigurnosna zaštita između dviju krajnjih točaka. VPN koristi ili RSA način potpisa ili unaprijed podijeljeni ključ za provjeru autentičnosti pregovora faze 1, kao i za uspostavljanje ključeva koji štite IKE poruke koje protječu za vrijeme narednih pregovora faze 2.

Unaprijed podijeljeni ključ je netrivijalan niz dužine do 128 znakova. Oba kraja veze se moraju složiti odijeljenom ključu. Prednost korištenja dijeljenih ključeva je njihova jednostavnost, mana je da dijeljena tajna mora biti distribuirana out-of-band, na primjer preko telefona ili preko registrirane pošte, prije IKE pregovora. Odnosite se prema svom dijeljenom ključu kao prema lozinci.

Provjera autentičnosti *RSA Potpis* daje više sigurnosti nego unaprijed podijeljeni ključ, zato što ovaj način koristi certifikate da omogući provjeru autentičnosti. Morate konfigurirati vaše digitalne certifikate preko Upravitelja digitalnim certifikatima. Dodatno, neka VPN rješenja zahtijevaju RSA Potpis za međuoperabilnost. Na primjer, Windows 2000 VPN koristi RSA potpis kao default metodu provjere autentičnosti. Konačno, RSA Potpis daje veću skalabilnost nego unaprijed podijeljeni ključevi. Certifikati koje koristite moraju dolaziti od izdavača certifikata kojem oba poslužitelja ključeva vjeruju.

Faza 2 Faza 2, međutim, pregovara sigurnosne asocijacije i ključeve koji će štititi stvarnu razmjenu aplikacijskih podataka. Zapamtite, do ove točke još nikakvi aplikacijski podaci zapravo nisu poslani. Faza 1 štiti IKE poruke faze 2.

Jednom kad su pregovori faze 2 dovršeni, vaš VPN uspostavlja sigurnu, dinamičku vezu preko mreže i između krajnjih točaka koje ste definirali za vašu vezu. Svi podaci koji teku preko VPN-a su dostavljeni s određenim stupnjem sigurnosti i efikasnosti koja je dogovorena preko poslužitelja ključa za vrijeme procesa pregovaranja faze 1 i faze 2.

Općenito, pregovori faze 1 se dogovaraju jednom na dan, dok se pregovori faze 2 osvježavaju svakih 60 minuta ili čak do svakih 5 minuta. Veće brzine osvježavanja povećavaju sigurnost vaših podataka, ali smanjuju performanse sistema. Koristite kratka vremena života ključa da zaštitite vaše najosjetljivije podatke.

Dinamički VPN možete kreirate korištenjem System i Navigator, morate definirati IKE politiku za omogućavanje pregovora faze 1 i politiku podataka za pregovore faze 2. Opcijski, možete koristiti čarobnjaka Nova veza. Čarobnjak automatski kreira svaki od konfiguracijskih objekata koje VPN zahtijeva za ispravan rad, uključujući IKE politiku, politiku podataka.

Preporučena literatura

Ako želite pročitati više o protokolu Internet razmjene ključeva (IKE) i upravljanju ključevima, pregledajte ove Internet Engineering Task Force (IETF) Zahtjeve za komentarima (RFC):

- RFC 2407, *Internet IP sigurnosna domena interpretacije ISAKMP*
- RFC 2408, *Internet sigurnosna asocijacija i Protokol upravljanja ključem (ISAKMP)*
- RFC 2409, *Internet Key Exchange (IKE)*

Pregledajte ove RFC-eve na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Srodni koncepti

“Scenarij: VPN naklonjen vatrozidu” na stranici 27
U ovom scenariju, veliko osiguravajuće poduzeće želi uspostaviti VPN između gatewaya u Chicagu i hosta u Minneapolisu, a obje mreže su iza vatrozida.

“IP Sigurnosni protokoli” na stranici 2
IP Sigurnost (IPSec) osigurava stabilnu, dugotrajnu bazu za osiguravanje sigurnosti mrežnog sloja.

Srodni zadaci

“Konfiguriranje politike Internet razmjene ključa” na stranici 45
Politika Internet razmjene ključa (IKE) definira koju razinu provjere autentičnosti i zaštite šifriranja IKE koristi za vrijeme faze 1 dogovora.

“Konfiguriranje politike podataka” na stranici 46
Politika podataka definira koja razina provjere autentičnosti ili šifriranja štiti podatke dok protječu kroz VPN.

Srodne informacije

http://www.rfc-editor.org

Protokol tunela sloja 2

Veze Protokola tunela sloja 2 (L2TP), koje su nazvane i virtualne linije, osiguravaju isplativiji pristup udaljenim korisnicima dopuštajući sistemima korporativne mreže da upravljaju IP adresama koje su dodijeljene njihovim udaljenim korisnicima. Nadalje, L2TP veze omogućuju siguran pristup vašem sistemu ili mreži kada ih koristite u spoju s protokolom IP sigurnosti (IPSec).

L2TP podržava dva tunelska načina: dobrovoljni tunel i prisilni tunel. Najveća razlika između ova dva tunelska načina je u krajnjoj točki. Na dobrovoljnom tunelu, tunel završava kod udaljenog klijenta dok prisilni tunel završava kod Internet dobavljača servisa (ISP).

S L2TP **prisilnim tunelom**, udaljeni host započinje vezu na svoj ISP. ISP zatim uspostavlja L2TP vezu između udaljenog korisnika i korporativne mreže. Iako ISP uspostavlja vezu, vi odlučujete kako zaštiti promet kod korištenja VPN-a. Kod prisilnog tunela ISP mora podržavati LT2P.

S L2TP **dobrovoljnim tunelom** veza je kreirana od udaljenog korisnika, najčešće upotrebom L2TP klijenta tuneliranja. Kao rezultat, udaljeni korisnik šalje L2TP pakete svom ISP-u, koji ih dalje prosljeđuje na korporativnu mrežu. S dobrovoljnim tunelom, ISP ne treba podržavati L2TP. Scenarij, zaštita L2TP tunela s IPSec vam daje primjer konfiguriranja sistema područnog ureda za spajanje s mrežom poduzeća preko gateway sistema s L2TP tunelom koji je zaštićen VPN-om.

Pogledajte vizualnu prezentaciju koncepta L2TP tunela koje štiti IPSec. Ovo zahtijeva Flash plug-in. Alternativno možete koristiti HTML verziju ove prezentacije.

L2TP je ustvari varijacija IP protokola sažimanja. L2TP tunel kreiran je sažimanjem L2TP okvira unutar paketa Protokola korisničkog datograma (UDP), koji se zauzvrat sažima unutar IP paketa. Adrese izvora i odredišta ovog IP paketa definiraju krajnje točke veze. Zato što je vanjski sažimajući protokol IP, možete primijeniti IPSec protokole na sastavljene IP pakete. Ovo zaštićuje podatke koji teku unutar L2TP tunela. Zatim možete primijeniti protokole Zaglavlje za provjeru autentičnosti (AH), Sažimanje tereta sigurnosti (ESP) i Internet razmjena ključa (IKE) na jednostavan način.

Srodni koncepti

“Scenarij: Zaštita L2TP dobrovoljnog tunela uz IPSec” na stranici 21
U ovom scenariju, naučite kako postaviti vezu između hosta područnog ureda i korporativnog ureda koji koristi L2TP koji štiti IPSec. Područni ured ima dinamički dodijeljenu IP adresu, dok korporativni ured ima statičku, globalno usmjerljivu IP adresu.

Prijevod mrežne adrese za VPN

VPN daje načine izvođenja prevođenja mrežnih adresa, zvanih VPN NAT. VPN NAT se razlikuje od tradicionalnog NAT-a u tome što prevodi adrese prije nego primjeni IKE i IPSec protokole. Obratite se na ovo poglavlje da naučite više.

Prijevod mrežne adrese (NAT) uzima vaše privatne IP adrese i prevodi ih u javne IP adrese. Ovo pomaže u očuvanju vrijednih IP adresa, dok u isto vrijeme dozvoljava hostovima na vašoj mreži pristup uslugama i udaljenim hostovima širom Interneta (ili neke druge javne mreže).

Dodatno, ako koristite privatne IP adrese, one se mogu sudariti sa sličnim, ulaznim IP adresama. Na primjer, možda ćete željeti komunicirati s drugom mrežom, ali obje mreže koriste 10.*.*.* adrese, uzrokujući da sve adrese kolidiraju i da se svi paketi ispuste. Primjena NAT-a na vaše odlazne adrese može izgledati kao rješenje vaših problema. Međutim, ako je promet podataka zaštićen od VPN-a, konvencionalni NAT neće raditi jer mijenja IP adrese u sigurnosnim asocijacijama (SA) koje VPN zahtijeva za funkcioniranje. Da izbjegnete ovaj problem, VPN omogućuje svoju vlastitu verziju prijevoda mrežne adrese, VPN NAT. VPN NAT obavlja prijevod adresa prije SA provjere valjanosti, dodjelom adrese vezi kada se veza pokrene. Adresa ostaje pridružena vezi sve dok ne obrišete vezu.

Bilješka: FTP trenutno ne podržava VPN NAT.

Kako mogu koristiti VPN NAT?

Dva su različita tipa VPN NAT-a koja trebate razmotriti prije nego započnete. To su:

VPN NAT za sprečavanje sukoba IP adresa

Ovaj tip VPN NAT-a vam dozvoljava da izbjegnete moguće sukobe IP adresa kada konfigurirate VPN vezu između mreža ili sistema sa sličnim shemama adresiranja. Tipični scenarij je onaj gdje oba poduzeća žele kreirati VPN veze koristeći jedan od predloženih raspona privatnih IP adresa. Na primjer, 10.*.*.*. Kako konfigurirate ovaj tip VPN NAT-a, ovisi o tome je li vaš sistem inicijator ili odgovaratelj za VPN vezu. Kada je vaš sistem inicijator veze, možete prevesti vaše lokalne adrese u one koje su kompatibilne s adresom VPN veze vašeg partnera. Kada je vaš sistem odgovaratelj na vezu, možete prevesti udaljene adrese vaših VPN partnera u one koje su kompatibilne sa shemom vašeg lokalnog adresiranja. Konfigurirajte ovaj tip prijevoda adresa samo za vaše dinamičke veze.

VPN NAT za skrivanje lokalnih adresa

Ovaj tip VPN NAT-a koristi se primarno za sakrivanje stvarne IP adrese vašeg lokalnog sistema, prevođenjem njegove adrese u drugu adresu koju ste učinili javno dostupnom. Kada konfigurirate

VPN NAT, možete navesti da svaka javno poznata IP adresa bude prevedena u jednu od onih iz spremišta sakrivenih adresa. Ovo vam također dozvoljava da uravnotežite punjenje prometa za individualnu adresu među više adresa. VPN NAT za lokalne adrese zahtijeva da vaš sistem radi kao odgovaratelj za svoje veze.

Koristite VPN NAT za sakrivanje lokalnih adresa ako odgovorite s 'da' na ova pitanja:

1. Imate li jedan ili više sistema kojima želite da ljudi pristupe preko VPN-a?
2. Trebate li biti fleksibilni oko stvarnih IP adresa vašeg sistema?
3. Da li imate jednu ili više globalno usmjerljivih IP adresa?

Scenarij, Upotreba prijevoda mrežne adrese za VPN vam daje primjer kako konfigurirati VPN NAT za skrivanje lokalnih adresa na vašem System i modelu.

Za korak-po-korak upute o postavljanju VPN NAT-a na sistemu, koristite online pomoć koja je dostupna iz VPN sučelja u System i Navigator.

Srodni koncepti

"Scenarij: Upotreba prijevoda mrežne adrese za VPN" na stranici 38
U ovom scenariju, poduzeće želi razmijeniti osjetljive podatke s jednim od poslovnih partnera koristeći VPN. Da bi se zaštitila privatnost mrežne strukture poduzeća, vaše poduzeće će također koristiti VPN NAT za skrivanje IP adresa sistema koje koristi za host aplikacija i na kojem poslovni partner ima pristup.

"Planiranje radne tablice za ručna povezivanja" na stranici 43
Dovršite ovu radnu tablicu prije konfiguriranja ručnog povezivanja.

NAT kompatibilni IPSec s UDP

UDP dozvoljava IPSec prometu da prođe kroz konvencionalan NAT uređaj. Pregledajte ovo poglavlje za više informacija o tome što je to i zašto bi ga koristili za vaše VPN veze.

Problem: Konvencionalni NAT prekida VPN

Prijevod mrežne adrese (NAT) vam dozvoljava da sakrijete vaše neregistrirane privatne IP adrese iza skupa registriranih IP adresa. Ovo vam pomaže u zaštiti vaše interne mreže od vanjskih mreža. NAT također pomaže u ublažavanju problema ispuštanja IP adrese, s obzirom da mnoge privatne adrese mogu biti predstavljene kao registrirane adrese.

Nažalost, konvencionalni NAT ne radi na IPSec paketima, jer kada paket ide kroz NAT uređaj, adresa izvora u paketu se mijenja i time čini paket nevažećim. Kada se to dogodi, kraj VPN veze koji je primalac odbacuje paket i pregovori za VPN vezu završavaju neuspjehom.

Rješenje: UDP sažimanje

U ljusci, UDP sažimanje sažima IPSec paket unutar novog, ali duplog, IP/UDP zaglavlja. Adresa u novom IP zaglavlju prevodi se kada ide kroz NAT uređaj. Tada, kad paket stigne na svoje odredište, primatelj skida konvencionalno zaglavlje, ostavljajući originalni IPSec paket, koji će sad proći sve ostale provjere.

UDP sažimanje možete primijeniti samo na VPN-ove koji će koristiti IPSec ESP bilo u tunelskom ili transportnom načinu. Dodatno, sistem može raditi samo kao klijent za UDP sažimanje. Odnosno, on može samo *inicirati* UDP sažeti promet.

Donja grafika ilustrira format UDP sažetog ESP paketa u tunelskom načinu:

Originalni IPv4 datogram:

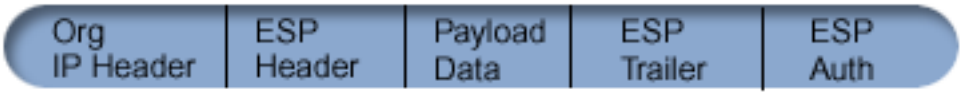
Nakon primjene IPSec ESP u tunel načinu:

Nakon primjene UDP sažimanja:

Donja grafika ilustrira format UDP sažetog ESP paketa u transportnom načinu:

Originalni IPv4 datogram:

Nakon primjene IPSec ESP u transport načinu:



Nakon primjene UDP sažimanja:

Nakon sažimanja paketa, sistem šalje paket do svog VPN partnera preko UDP porta 4500. Tipično, VPN partneri obavljaju IKE pregovore preko UDP porta 500. Pa ipak, kada IKE otkrije NAT u toku pregovora oko ključa, sljedeći IKE paketi se šalju preko izvorišnog porta 4500, na odredišni port 4500. Ovo također znači da port 4500 mora biti neograničen u bilo kojem primjenjivom pravilu filtera. Primatelj na vezi može tada odrediti da li je paket IKE paket ili UDP sažeti paket, jer prvih 4 bajta UDP opterećenja su postavljeni na nula u IKE paketu. Da to radi ispravno, oba kraja veze moraju podržavati UDP sažimanje.

Srodni koncepti

“Scenarij: VPN naklonjen vatrozidu” na stranici 27
U ovom scenariju, veliko osiguravajuće poduzeće želi uspostaviti VPN između gatewaya u Chicagu i hosta u Minneapolisu, a obje mreže su iza vatrozida.

IP komprimiranje

Protokol IP komprimiranja tereta (IPComp) smanjuje veličinu IP datograma komprimiranjem datograma da se povećaju performanse komunikacija između dva partnera.

Namjera je da se ukupno povećaju performanse komunikacije kada komunikacija ide preko sporih ili zagušenih veza. IPComp ne omogućuje bilo kakvu sigurnost i mora biti korišteno zajedno s AH ili ESP pretvorbom kada se komunikacija odvija preko VPN veze.

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira IPComp u zahtjevu za komentarima (RFC) 2393, *Protokol IP komprimiranja tereta (IPComp)*. Pregledajte ovaj RFC na Internetu na sljedećoj Web stranici: http://www.rfc-editor.org.

Srodne informacije

http://www.rfc-editor.org

VPN i IP filtriranje

IP filtriranje i VPN blisko su povezani. Zapravo, većina VPN veza zahtijeva pravila filtriranja za ispravan rad. Ovo poglavlje daje vam informacije o tome koje filtere VPN zahtijeva, kao i ostale koncepte filtriranja povezane s VPN-om.

Većina VPN veza zahtijeva pravila filtriranja za ispravan rad. Zahtijevana pravila filtriranja ovise o tipu VPN veze koju konfigurirate, kao i o tipu prometa koji želite kontrolirati. Općenito, svaka veza će imati filter politike. Filter politike definira koje adrese, protokoli i portovi mogu koristiti VPN. Dodatno, veze koje podržavaju protokol Internet Razmjene Ključeva (IKE) obično imaju pravila koja su napisana izričito da dozvole IKE obradu preko veze. VPN može automatski generirati ova pravila. Kada je god moguće, dozvolite VPN-u da generira za vas vaše filtere politika. Ovo neće samo pomoći eliminirati greške, nego i potrebu za konfiguracijom pravila kao poseban korak korištenjem editora Pravila paketa u System i Navigator.

Naravno, postoje i izuzeci. Pregledajte ova poglavlja da naučite više o drugim, manje uobičajenim VPN i konceptima filtriranja i tehnikama koje se mogu primijeniti na vašu konkretnu situaciju:

Srodni koncepti

“Konfiguriranje VPN paketnih pravila” na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

VPN veze bez filtera politike

Ako su krajnje točke veze vašeg VPN-a jednostruke, specifične IP adrese i vi želite pokrenuti VPN bez potrebe da napišete ili aktivirate pravila filtriranja na sistemu, možete konfigurirati dinamički filter politike.

Filter politike definira koje adrese, protokoli i portovi mogu koristiti VPN i usmjerava prikladan promet preko te veze. U nekim slučajevima ćete možda željeti konfigurirati vezu koja ne zahtijeva politiku pravila filtera. Na primjer, možda ćete imati ne-VPN paket pravila učitan na sučelju koje će vaša VPN veza koristiti, pa radije nego da deaktivirate aktivna pravila na tom sučelju, odlučite konfigurirati VPN tako da vaš sistem upravlja sve filtere dinamički za vezu. Filter politike za ovaj tip veze naziva se **dinamički filter politike**. Prije nego možete koristiti dinamički filter politike za vašu VPN vezu, svaka od sljedećih stavki mora biti istinita:

- Veza se može započeti samo preko lokalnog sistema.
- Krajnje točke podataka za vezu moraju biti jednostruki sistemi. To znači, one ne mogu biti podmreža ili raspon adresa.
- Niti jedno pravilo filtriranja politike ne može biti učitano za vezu.

Ako vaša veza ispunjava ove kriterije, možete konfigurirati vezu tako da ne zahtijeva filter politike. Kada se pokrene veza, promet između krajnjih točaka podataka će protjecati preko nje bez obzira koja su druga paketna pravila učitana na vaš sistem.

Za upute korak po korak kako konfigurirati vezu tako da ne zahtijeva filter politike, koristite online sistem pomoći za VPN.

Uključeni IKE

Da bi se dogovori za Razmjenu Internet ključa (IKE) desili za vaš VPN, trebate omogućiti UDP datograme preko porta 500 za ovaj tip IP prometa. Međutim, ako nema pravila filtriranja na sistemu specifično napisanih sa svrhom dozvole IKE prometa, tada će sistem uključivo dozvoliti protok IKE prometa.

Za postavljanje veze, većina VPN-ova zahtijeva da se IKE dogovori ostvare prije nego se desi IPSec obrada. IKE koristi dobro poznati port 500. Zato, da bi IKE radio ispravno, trebate dozvoliti UDP datograme preko porta 500 za ovaj tip IP prometa. Ako nema pravila filtriranja na sistemu napisanih sa svrhom dozvole IKE prometa, tada je IKE promet uključeno dozvoljen. Pa ipak, pravilima pisanim baš za promet na UDP portu 500 se rukuje ovisno o tome što je definirano u aktivnim pravilima filtera.

Scenariji: VPN

Pregledajte ove scenarije kako biste postali upoznati s tehničkim i konfiguracijskim detaljima uključeni u svaki od ovih osnovnih tipova veze.

Srodni koncepti

QoS scenarij: Sigurni i predvidljivi rezultati (VPN i QoS)

Srodne informacije

OS/400 V5R1 Virtualne privatne mreže: Udaljeni pristup na IBM e(logo)server iSeries poslužitelj s Windows 2000 VPN klijentima, REDP0153

AS/400 Internet sigurnost: Implementacija AS/400 Virtualnih privatnih mreža, SG24-5404-00

AS/400 Scenariji Internet sigurnosti: Praktični pristup, SG24-5954-00

Scenarij: Osnovno povezivanje područnog ureda

U ovom scenariju, vaše poduzeće želi postaviti VPN između podmreža dvaju udaljenih odjela preko para System i modela koji djeluju kao VPN prilazi.

Situacija

Pretpostavite da vaše poduzeće želi smanjiti troškove kojima se izvrgava zbog komunikacije sa i između svojih podružnica. Danas vaše poduzeće koristi frame relay ili iznajmljene linije, ali vi želite istražiti druge opcije za prenošenje internih povjerljivih podataka koje su manje skupe, sigurnije i globalno pristupačne. Iskorištavanjem Interneta možete lako uspostaviti virtualnu privatnu mrežu (VPN) koja će odgovarati potrebama vašeg poduzeća.

Vaše poduzeće i njegov područni ured oboje trebaju VPN zaštitu preko Interneta, ali ne i unutar njihovih intraneta. Zato što intranete smatrate sigurnima, najbolje je rješenje kreiranje prilaz-prilaz VPN-a. U ovom slučaju oba prilaza direktno su povezana na posredničku mrežu. Drugim riječima, oni su *granični* ili *rubni* sistemi koji nisu zaštićeni vatrozidom. Ovaj primjer služi kao koristan uvod u korake uključene u postavljanje osnovne VPN konfiguracije. Kada se ovaj scenarij odnosi na termin *Internet*, odnosi se na prijenosnu mrežu između dva VPN prilaza, koja može biti privatna mreža poduzeća ili javni Internet.

Važno: Ovaj scenarij pokazuje System i model sigurnosnih prilaza dodanih direktno na Internet. Nepostojanje vatrozida je zbog jednostavnosti scenarija. To ne znači da upotreba vatrozida nije potrebna. U stvari, uzmite u obzir sigurnosne mjere svaki put kad se povezujete na Internet.

Prednosti

Ovaj scenarij ima sljedeće prednosti:

- Korištenje Interneta ili postojećeg intraneta smanjuje troškove privatnih linija između udaljenih podmreža.
- Korištenje Interneta ili postojećeg intraneta smanjuje kompleksnost instaliranja i održavanja privatnih linija i pridružene opreme.
- Korištenje Interneta dozvoljava udaljenim lokacijama povezivanje gotovo bilo gdje na svijetu.
- Upotreba VPN-a osigurava korisnicima pristup svim sistemima i resursima na strani povezivanja kao i tamo gdje su se povezali upotrebom veze preko unajmljene linije ili mreže širokog područja (WAN).
- Upotreba industrijskog standardnog šifriranja i metoda provjere autentičnosti osigurava sigurnost osjetljivih informacija koje se predaju s jedne lokacije na drugu.
- Redovita i dinamička zamjena vaših ključeva pojednostavljuje postav i smanjuje rizik da vaši ključevi budu dekodirani, odnosno da vaša sigurnost bude razbijena.
- Koristeći privatne IP adrese u svakoj udaljenoj podmreži čini nepotrebnim dodjelu vrijednih javnih IP adresa svakom klijentu.

Ciljevi

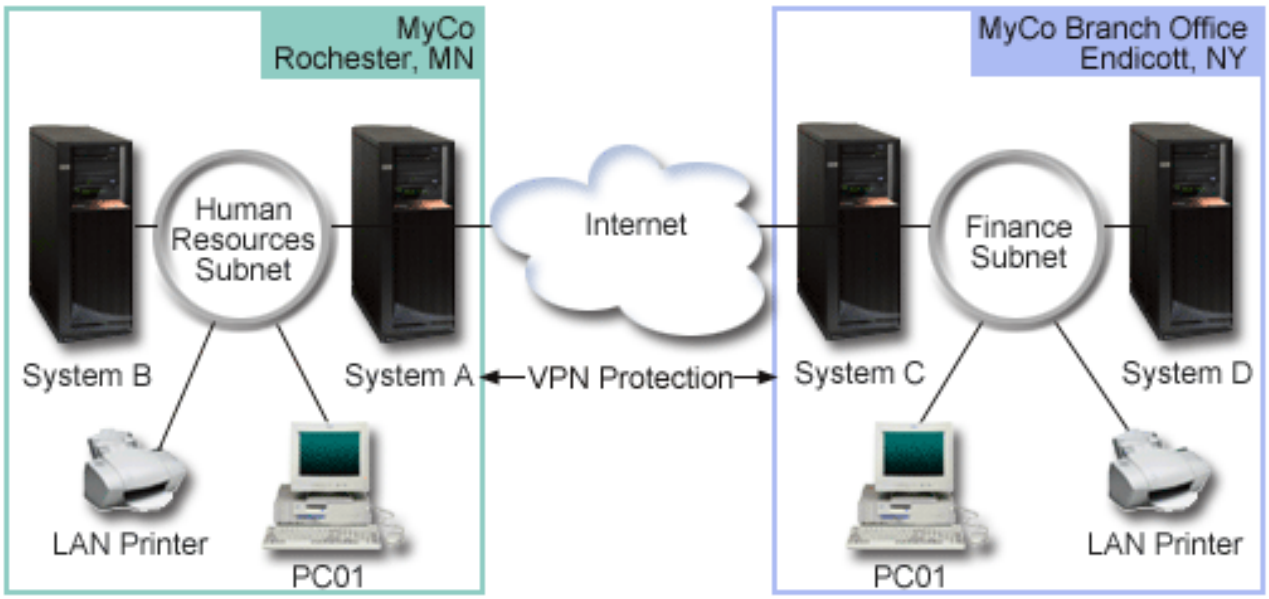
U ovom scenariju, MyCo, Inc. želi postaviti VPN između podmreža svojih odjela Ljudskih resursa i Financija preko para System i modela. Oba sistema će raditi kao VPN prilazi. U uvjetima VPN konfiguracija, prilaz obavlja ključno upravljanje i primjenjuje IPSec na podatke koji protječu kroz tunel. Prilazi nisu krajnje točke veze za podatke.

Ciljevi ovog scenarija su sljedeći:

- VPN mora štititi sav promet podataka između podmreže odjela za Ljudske resurse i podmreže odjela za Financije.
- Promet podataka ne zahtijeva VPN zaštitu jednom kad dosegne bilo koju od podmreža ovih odjela.
- Svi klijenti i hostovi na svakoj mreži imaju potpuni pristup na mrežu onog drugog, uključujući sve aplikacije.
- Sistemi prilaza mogu komunicirati jedan s drugim i pristupiti međusobnim aplikacijama.

Detalji

Sljedeća slika ilustrira karakteristike mreže od MyCo.



Odjel ljudskih resursa

- Sistem A se izvodi na i5/OS verziji 5 izdanju 3 (V5R3) ili kasnijem i radi kao VPN prilaz Odjela ljudskih resursa.
- Podmreža je 10.6.0.0 s maskom 255.255.0.0. Ova podmreža za podatke predstavlja krajnju točku VPN tunela na MyCo Rochester stranici.
- Sistem A se spaja na Internet s IP adrese 204.146.18.227. Ovo je krajnja točka veze. To znači da Sistem A obavlja upravljanje ključem i primjenjuje IPSec na dolazne i izlazne IP datograme.
- Sistem A se povezuje na svoju podmrežu s IP adresom 10.6.11.1.
- Sistem B je proizvodni sistem u podmreži Ljudski resursi koja izvodi standardne TCP/IP aplikacije.

Odjel za financije

- Sistem C se izvodi na i5/OS verziji 5 izdanju 3 (V5R3) ili kasnijem, i radi kao VPN prilaz Odjela financija.
- Podmreža je 10.196.8.0 s maskom 255.255.255.0. Ova podmreža za podatke predstavlja krajnju točku VPN tunela na MyCo Endicott stranici.
- Sistem C se spaja na Internet s IP adresom 208.222.150.250. Ovo je krajnja točka veze. To znači da System C obavlja upravljanje ključem i primjenjuje IPSec na dolazne i izlazne IP datograme.
- Sistem C se spaja na svoju podmrežu s IP adresom 10.196.8.5.

Zadaci konfiguracije

Morate dovršiti svaki od ovih zadataka da konfigurirate povezivanje područnog ureda opisano u ovom scenariju:

Bilješka: Prije pokretanja ovih zadataka provjerite TCP/IP usmjeravanje da osigurate da dva sistema prilaza mogu komunicirati jedan s drugim preko Interneta. Ovo osigurava da se hostovi na svakoj podmreži ispravno usmjeravaju na njihov odgovarajući prilaz za pristup udaljenoj podmreži.

Srodni koncepti

TCP/IP usmjeravanje i ravnoteža radnog opterećenja

Srodne informacije

AS/400 Scenariji Internet sigurnosti: Praktični pristup, SG24-5954-00

Dovršenje radne tablice planiranja

Kontrolne liste planiranja ilustriraju tip informacija koje trebate prije početka konfiguriranja VPN-a. Svi odgovori na preduvjetnoj kontrolnoj listi moraju biti DA prije nego nastavite s postavljanjem VPN-a.

Bilješka: Ove radne tablice se primjenjuju na Sistem A, ponavljaju obradu za Sistem C, vraćajući IP adrese, prema potrebi.

Tablica 1. Sistemski zahtjevi

Kontrolna lista preduvjeta	**Odgovori**
Izvodi li sistem i5/OS V5R3, ili kasniju?	Da
Je li Upravitelj digitalnih certifikata opcija instalirana?	Da
Da li je instaliran System i Access za Windows?	Da
Da li je instaliran System i Navigator?	Da
Da li je instalirana mrežna pomoćna komponenta System i Navigator ?	Da
Da li je instaliran IBM TCP/IP pomoćni programi povezanosti za i5/OS?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na sistemu (uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene)?	Da
Da li je uspostavljena normalna TCP/IP komunikacija između zahtijevanih krajnjih točaka?	Da
Jeste li primijenili privremene popravke za posljednji program (PTF-ove)?	Da
Ako VPN tunel prolazi kroz vatrozid ili usmjerivače koji koriste IP filtriranje, da li pravila filtriranja vatrozida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatrozidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	Da
Da li su vatrozidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Tablica 2. VPN konfiguracija

Ove informacije trebate za konfiguraciju VPN-a	**Odgovori**
Koji tip veze kreirate?	prilaz-prilaz
Kako ćete nazvati grupu dinamičkog ključa?	HRgw2FINgw
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših ključeva?	uravnoteženi
Da li koristite certifikate za provjeru autentičnosti veze? Ako ne, koji je unaprijed podijeljeni ključ?	Bez vrhunskih tajni
Koji je identifikator za lokalnog poslužitelja ključa?	IP adresa: 204.146.18.227

Tablica 2. VPN konfiguracija (nastavak)

Ove informacije trebate za konfiguraciju VPN-a	**Odgovori**
Koji je identifikator za lokalnu krajnju točku podataka?	Podmreža: 10.6.0.0 Maska: 255.255.0.0
Koji je identifikator udaljenog poslužitelja ključa?	IP adresa: 208.222.150.250
Koji je identifikator za udaljenu krajnju točku podataka?	Podmreža: 10.196.8.0 Maska: 255.255.255.0
Koje portove i protokole želite dozvoliti za protok vezom?	Bilo koje
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka?	uravnoteženi
Na koja se sučelja veza odnosi?	TRLINE

Konfiguriranje VPN-a na Sistemu A

Dovršite ovaj zadatak za konfiguraciju Sistema A

Koristite sljedeće korake i informacije iz vaših radnih tablica za konfiguraciju VPN-a na Sistemu A:

1. U System i Navigator, proširite **Sistem A → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete Čarobnjaka za novu vezu.
3. Pregledajte stranicu **Pozdrav** za informacije o objektima koje kreira čarobnjak.
4. Kliknite **Sljedeće** za odlazak na stranicu **Ime veze**
5. U polje **Ime** unesite HRgw2FINgw.
6. Opcijski: Navedite opis ove grupe veza.
7. Kliknite **Sljedeće** za odlazak na stranicu **Scenario veze**.
8. Izaberite **Povežite vaš prilaz na drugi prilaz**.
9. Kliknite **Sljedeće** za odlazak na stranicu **Politika razmjene Internet ključeva.**
10. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.
11. Kliknite **Sljedeće** za odlazak na stranicu **Certifikat za krajnju točku Lokalne veze**.
12. Izaberite **Ne** da označite da nećete koristiti certifikate za provjeru autentičnosti veze.
13. Kliknite **Sljedeće** da odete na stranicu **Lokalni poslužitelj ključeva**.
14. Izaberite **IP adresa Verzija 4** iz polja **Tip identifikatora**.
15. Izaberite 204.146.18.227 iz polja **IP adresa**.
16. Kliknite **Sljedeće** za odlazak na stranicu **Udaljeni poslužitelj s ključevima**.
17. Izaberite **IP adresa verzija 4** u polju **Tip identifikatora.**
18. Upišite 208.222.150.250 u polju **Identifikator**.
19. Unesite topsecretstuff u polju **Preddijeljeni ključ**
20. Kliknite na **Sljedeće** da odete na stranicu **Lokalna krajnja točka podataka**.
21. Izaberite **IP verzija 4 podmreža** iz polja **Tip identifikatora**.
22. Upišite 10.6.0.0 u polju **Identifikator**.
23. Upišite 255.255.0.0 u polju **Maska podmreže**.
24. Kliknite na **Sljedeće** da odete na stranicu **Udaljena krajnja točka podataka**.
25. Izaberite **Podmreža IP verzije 4** s polja **Tip identifikatora**
26. Upišite 10.196.8.0 u polju **Identifikator**.
27. Upišite 255.255.255.0 u polju **Maska podmreže**.
28. Kliknite na **Sljedeće** da odete na stranicu **Usluge podataka**.
29. Prihvatite defaultne vrijednosti i kliknite na **Sljedeće** za odlazak na stranicu **Politike podataka**.

30. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.
31. Izaberite **Koristi algoritam šifriranja RC4**.
32. Kliknite **Sljedeće** za odlazak na stranicu **Primjenjiva sučelja**.
33. Izaberite **TRLINE** iz tablice **Linija**.
34. Kliknite **Sljedeće** za odlazak na stranicu **Sažetak.** Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.
35. Kliknite **Završetak** za dovršetak konfiguracije.
36. Kada se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Da, aktiviraj generirane filtere politike**, tada izaberite **Dozvoli sav ostali promet**.
37. Kliknite **OK** da dovršite konfiguraciju. Kada bude zatraženo, navedite da želite aktivirati pravila na svim sučeljima.

Srodni zadaci

"Konfiguriranje VPN-a na Sistemu C"
Slijedite iste korake koje ste koristili za konfiguriranje VPN-a na Sistemu A, mijenjanjem IP adrese, po potrebi. Kao vodič koristit će vam planske radne tablice.

Konfiguriranje VPN-a na Sistemu C

Slijedite iste korake koje ste koristili za konfiguriranje VPN-a na Sistemu A, mijenjanjem IP adrese, po potrebi. Kao vodič koristit će vam planske radne tablice.

Kada završite konfigurirati VPN prilaz Odjela za financije, vaše veze će biti u stanju *on-demand*, što znači da se veza pokreće kada se pošalju IP datogrami koje VPN veza mora štititi. Sljedeći je korak pokretanje VPN poslužitelja, ako već nisu pokrenuti.

Srodni zadaci

"Konfiguriranje VPN-a na Sistemu A" na stranici 15
Dovršite ovaj zadatak za konfiguraciju Sistema A

VPN pokretanje

Nakon konfiguracije vaše VPN veze na Sistemu A i C, trebate pokrenuti vašu VPN vezu.

Da pokrenete VPN, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Pokreni**.

Testiranje veze

Nakon završetka konfiguracije oba sistema i uspješnog pokretanja VPN poslužitelja, testirajte povezanost da osigurate da udaljene podmreže mogu komunicirati jedna s drugom.

Za testiranje vaše veze, slijedite ove korake:

1. U System i Navigator, proširite **Sistem A → Mreža**.
2. Desno kliknite **TCP/IP Konfiguracija** i izaberite **Pomoćni programi** i nakon toga izaberite **Ping**.
3. Iz kućice dijaloga **Ping sa**, unesite Sistem C u polje **Ping**.
4. Kliknite **Ping sada** da provjerite povezanost od Sistema A do Sistema C.
5. Kliknite **OK** pri završetku.

Scenarij: Osnovno povezivanje posla s poslom

U ovom scenariju vaše poduzeće želi uspostaviti VPN između radne stanice klijenta u vašem proizvodnom odjelu i radne stanice klijenta u odjelu za nabavu vašeg poslovnog partnera.

Situacija

Mnoga poduzeća koriste frame relay ili iznajmljene linije da omoguće sigurnu komunikaciju sa svojim poslovnim partnerima, pomoćnicima i prodavačima. Nažalost, ova rješenja su najčešće skupa i geografski ograničavajuća. VPN daje alternativu za poduzeća koja žele privatnu, cijenom prihvatljivu komunikaciju.

Zamislite da ste glavni dobavljač dijelova za proizvođača. Obzirom da je od kritične važnosti da imate određene dijelove i količinu točno u trenutku zahtijevanom od poduzeća proizvođača, uvijek trebate biti svjesni stanja u inventaru proizvođača i rasporeda proizvodnje. Možda danas ovakvom interakcijom rukujete ručno i smatrate ju vremenski dugotrajnom, skupom, čak povremeno i netočnom. Htjeli biste pronaći lakši, brži i učinkovitiji način komuniciranja s vašim proizvodnim poduzećem. Međutim, s obzirom na povjerljivu prirodu i vremensku osjetljivost informacija koje izmjenjujete, proizvođač ih ne želi objaviti na svojim korporativnim Web stranicama ili ih distribuirati mjesečno u vanjskom izvještaju. Korištenjem javnog Interneta možete lako postaviti VPN da udovoljite potrebama oba poduzeća.

Ciljevi

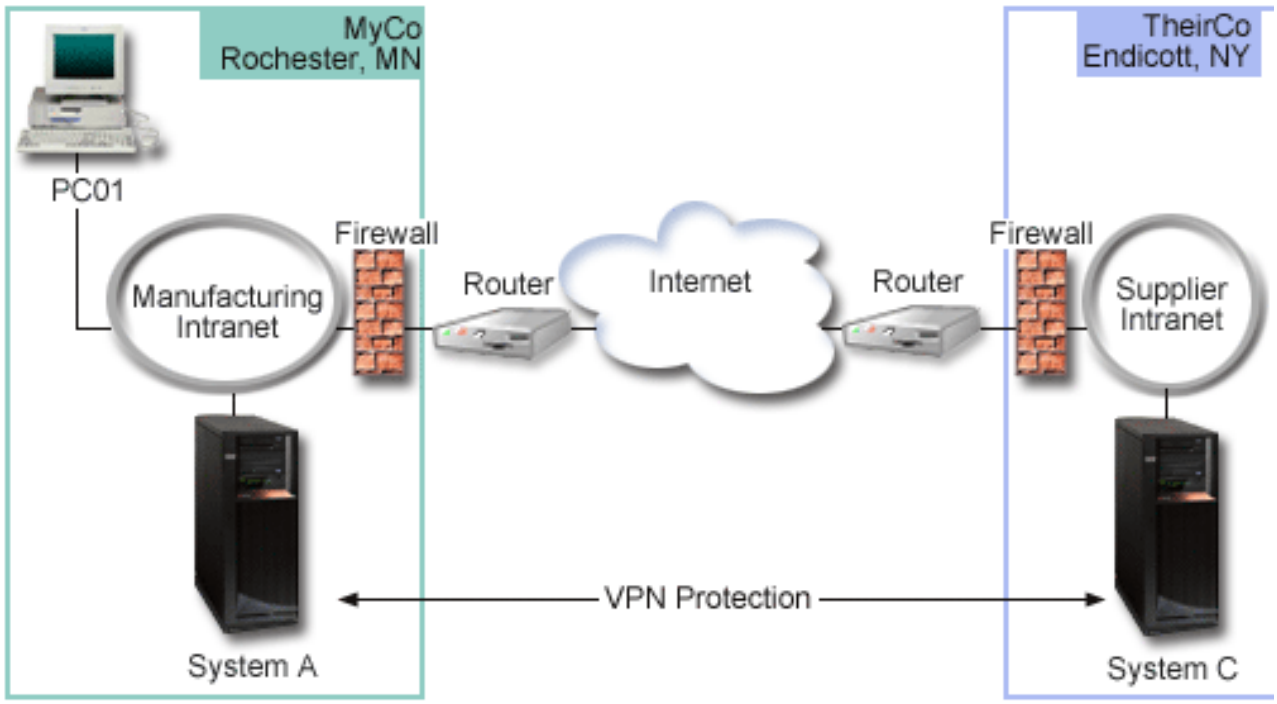
U ovom scenariju, MyCo želi uspostaviti VPN između hosta i njegovog odjela za dijelove i hosta u odjelu za proizvodnju jednog od njegovih poslovnih partnera, TheirCo.

Zbog toga što su informacije koje dijele ova dva poduzeća izuzetno povjerljive, moraju biti zaštićene dok putuju preko Interneta. Dodatno, podaci ne smiju teći nezaštićeno kroz mrežu oba poduzeća, jer svaka strana smatra drugu nepovjerljivom. Drugim riječima, oba poduzeća zahtijevaju provjeru autentičnosti od kraja do kraja, cjelovitost i šifriranje.

Važno: Namjera ovog scenarija je da primjerom predstavi jednostavnu host-host VPN konfiguraciju. U tipičnoj mrežnoj okolini također ćete, među ostalim, trebati razmotriti konfiguraciju vatrozida, zahtjeve IP adresiranja i usmjeravanje.

Detalji

Sljedeća slika ilustrira mrežne karakteristike od MyCo i TheirCo:



MyCo mreža za dobavljanje

- Sistem A se izvodi na i5/OS verziji 5 izdanje 3 (V5R3) ili kasnije.
- Sistem A ima IP adresu 10.6.1.1. Ovo je krajnja točka veze, odnosno krajnja točka za podatke. To znači da Sistem A obavlja IKE dogovaranja i primjenjuje IPSec na dolazne i izlazne IP datograme i izvor je i odredište podataka koji teku kroz VPN.
- Sistem A je u podmreži 10.6.0.0 s maskom 255.255.0.0
- Samo Sistem A može započeti vezu sa Sistemom C.

TheirCo mreža za proizvodnju

- Sistem C se izvodi na i5/OS verziji 5 izdanju 3 (V5R3) ili kasnijem.
- Sistem C ima IP adresu 10.196.8.6. Ovo je krajnja točka veze, odnosno krajnja točka za podatke. To znači da Sistem A obavlja IKE dogovaranja i primjenjuje IPSec na dolazne i izlazne IP datograme i izvor je i odredište podataka koji teku kroz VPN.
- Sistem C je podmreža 10.196.8.0 s maskom 255.255.255.0

Zadaci konfiguracije

Morate dovršiti svaki od ovih zadataka da konfigurirate posao-posao povezivanje opisano u ovom scenariju:

Bilješka: Prije pokretanja ovih zadataka provjerite TCP/IP usmjeravanje da osigurate da dva sistema prilaza mogu komunicirati jedan s drugim preko Interneta. Ovo osigurava da se hostovi na svakoj podmreži ispravno usmjeravaju na njihov odgovarajući prilaz za pristup udaljenoj podmreži.

Srodni koncepti

TCP/IP usmjeravanje i ravnoteža radnog opterećenja

Dovršenje radne tablice planiranja

Kontrolne liste planiranja ilustriraju tip informacija koje trebate prije početka konfiguriranja VPN-a. Svi odgovori na preduvjetnoj kontrolnoj listi moraju biti DA prije nego nastavite s postavljanjem VPN-a.

Bilješka: Ove radne tablice se primjenjuju na Sistem A, ponavljaju obradu za Sistem C, vraćajući IP adrese, prema potrebi.

Tablica 3. Sistemski zahtjevi

Kontrolna lista preduvjeta	**Odgovori**
Izvodi li sistem i5/OS V5R3, ili kasniju?	Da
Je li Upravitelj digitalnih certifikata opcija instalirana?	Da
Da li je instaliran System i Access za Windows?	Da
Da li je instaliran System i Navigator?	Da
Da li je instalirana mrežna pomoćna komponenta System i Navigator ?	Da
Da li je instaliran IBM TCP/IP pomoćni programi povezanosti za i5/OS?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na sistemu (uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene)?	Da
Da li je uspostavljena normalna TCP/IP komunikacija između zahtijevanih krajnjih točaka?	Da
Jeste li primijenili privremene popravke za posljednji program (PTF-ove)?	Da
Ako VPN tunel prolazi kroz vatrozid ili usmjerivače koji koriste IP filtriranje, da li pravila filtriranja vatrozida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatrozidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	Da
Da li su vatrozidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Tablica 4. VPN konfiguracija

Ove informacije trebate za konfiguraciju VPN-a	**Odgovori**
Koji tip veze kreirate?	prilaz-prilaz
Kako ćete nazvati grupu dinamičkog ključa?	HRgw2FINgw
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših ključeva?	uravnoteženi
Da li koristite certifikate za provjeru autentičnosti veze? Ako ne, koji je unaprijed podijeljeni ključ?	Bez vrhunskih tajni
Koji je identifikator za lokalnog poslužitelja ključa?	IP adresa: 204.146.18.227
Koji je identifikator za lokalnu krajnju točku podataka?	Podmreža: 10.6.0.0 Maska: 255.255.0.0
Koji je identifikator udaljenog poslužitelja ključa?	IP adresa: 208.222.150.250
Koji je identifikator za udaljenu krajnju točku podataka?	Podmreža: 10.196.8.0 Maska: 255.255.255.0
Koje portove i protokole želite dozvoliti za protok vezom?	Bilo koje
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka?	uravnoteženi
Na koja se sučelja veza odnosi?	TRLINE

Konfiguriranje VPN-a na Sistemu A

Dovršite sljedeće korake za konfiguriranje VPN veze na Sistemu A.

Koristite informacije iz vaših radnih tablica planiranja, da konfigurirate VPN na Sistemu A, kako slijedi:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete Čarobnjaka za vezu.
3. Pregledajte stranicu **Pozdrav** za informacije o objektima koje kreira čarobnjak.
4. Kliknite **Sljedeće** za odlazak na stranicu **Ime veze**
5. U polje **Ime** upišite MyCo2TheirCo.
6. Opcijski: Navedite opis ove grupe veza.
7. Kliknite **Sljedeće** za odlazak na stranicu **Scenarij veze.**
8. Izaberite **Povežite vaš host na drugi host**.
9. Kliknite **Sljedeće** za odlazak na stranicu **Politika razmjene Internet ključeva.**
10. Izaberite **Kreiranje nove politike** i zatim izaberite **Najveća sigurnost, najmanje performanse**.
11. Kliknite **Sljedeće** za odlazak na stranicu **Certifikat za krajnju točku Lokalne veze**.
12. Izaberite **Da** da naznačite da nećete koristiti certifikate za provjeru autentičnosti veze. Onda izaberite certifikat koji predstavlja Sistem A.

    Bilješka: Ako želite koristiti certifikat za provjeru autentičnosti krajnje točke lokalne veze, morate prvo kreirati certifikat u Upravitelju digitalnih certifikata (DCM).
13. Kliknite **Sljedeće** da odete na stranicu **Identifikator lokalne krajnje točke veze**.
14. Izaberite **IP adresa Verzija 4** kao tip identifikatora. Asocirana IP adresa mora biti 10.6.1.1. Ponavljamo, ove informacije su definirane u certifikatu koji kreirate u DCM-u.
15. Kliknite **Sljedeće** za odlazak na stranicu **Udaljeni poslužitelj s ključevima**.
16. Izaberite **IP adresa verzija 4** u polju **Tip identifikatora.**
17. Upišite 10.196.8.6 u polju **Identifikator**.
18. Kliknite na **Sljedeće** da odete na stranicu **Usluge podataka.**
19. Prihvatite defaultne vrijednosti i kliknite na **Sljedeće** za odlazak na stranicu **Politike podataka**.
20. Izaberite **Kreiranje nove politike** i zatim izaberite **Najveća sigurnost, najmanje performanse**. Izaberite **Koristite algoritam šifriranja RC4**.
21. Kliknite **Sljedeće** za odlazak na stranicu **Primjenjiva sučelja.**
22. Izaberite **TRLINE**.
23. Kliknite **Sljedeće** za odlazak na stranicu **Sažetak.** Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.
24. Kliknite **Završetak** za dovršetak konfiguracije.
25. Kada se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Ne, aktiviraj pravila paketa u neko drugo vrijeme**, tada izaberite **OK**.

Sljedeći korak je da specificirate da samo Sistem A može započeti ovu vezu. To napravite prilagođavanjem svojstava grupe dinamičkog ključa, MyCo2TheirCo, koju je kreirao čarobnjak:

1. Kliknite **Po grupi** u lijevom oknu VPN sučelja; nova grupa dinamičkog ključa, MyCo2TheirCo, prikazuje se u desnom oknu. Desno kliknite i izaberite **Svojstva**.
2. Otiđite na stranicu **Politika** i izaberite opciju **Lokalni sistem započinje vezu**.
3. Kliknite **OK** za spremanje promjena.

Konfiguriranje VPN-a na Sistemu C

Slijedite iste korake koje ste koristili za konfiguriranje VPN-a na Sistemu A, mijenjanjem IP adrese, po potrebi. Kao vodič koristit će vam planske radne tablice.

Kada završite konfigurirati VPN prilaz Odjela za financije, vaše veze će biti u stanju *on-demand*, što znači da se veza pokreće kada se pošalju IP datogrami koje VPN veza mora štititi. Sljedeći je korak pokretanje VPN poslužitelja, ako već nisu pokrenuti.

Aktiviranje paketnih pravila

VPN čarobnjak automatski kreira paketna pravila koje ova veza zahtijeva za ispravan rad. Međutim, njih morate aktivirati na oba sistema prije nego možete pokrenuti VPN vezu.

Da aktivirate paketna pravila na Sistemu A, slijedite ove korake:

1. U System i Navigator, proširite **Sistem A → Mreža → IP Politike**.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje paketnih pravila**.
3. Izaberite želite li aktivirati samo VPN generirana pravila, samo izabranu datoteku ili oboje, VPN generirana pravila i izabranu datoteku. Ovo posljednje biste mogli izabrati ako, na primjer, imate svakovrsna PERMIT i DENY pravila koja želite nametnuti sučelju kao dodatak VPN generiranim pravilima.
4. Izaberite sučelje na kojem želite aktivaciju pravila. U ovom slučaju, izaberite **Sva sučelja**.
5. Kliknite na **OK** u kućici dijaloga da potvrdite kako želite provjeriti i aktivirati pravila na sučelju ili sučeljima koje ste naveli. Nakon što kliknete OK, sistem provjerava pravila od sintaktičkih i semantičkih pogrešaka i daje izvještaj o rezultatima u prozoru za poruke na dnu editora. Za poruke o greškama koje se odnose na određenu datoteku ili broj linije, možete desno kliknuti na grešku i izabrati **Idi na liniju** da osvijetlite grešku u datoteci.
6. Ponovite ove korake da aktivirate paketna pravila na Sistemu C.

Pokretanje veze

Nakon konfiguracije vaše VPN veze, trebate pokrenuti vašu VPN vezu.

Slijedite ove korake za pokretanje MyCo2TheirCo veze sa Sistema A:

1. U System i Navigator, proširite **Sistem A → Mreža → IP politike**.
2. Ako VPN poslužitelj nije pokrenut, desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Pokreni**. Ovo pokreće VPN poslužitelj.
3. Proširite **Virtualno privatno umrežavanje → Sigurne veze**.
4. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
5. Desno kliknite **MyCo2TheirCo** i izaberite **Pokreni**.
6. Iz izbornika **Pogled** izaberite **Osvježi**. Ako se veza uspješno uspostavi, status će se promijeniti iz *Mirovanja* na *Omogućeno*. Pokretanje veze može trajati nekoliko minuta, pa povremeno napravite osvježavanje dok se status ne promijeni u *Omogućeno*.

Testiranje veze

Nakon završetka konfiguracije oba sistema i uspješnog pokretanja VPN poslužitelja, testirajte povezanost da osigurate da udaljene podmreže mogu komunicirati jedna s drugom.

Za testiranje vaše veze, slijedite ove korake:

1. U System i Navigator, proširite **Sistem A → Mreža**.
2. Desno kliknite **TCP/IP Konfiguracija** i izaberite **Pomoćni programi** i nakon toga izaberite **Ping**.
3. Iz kućice dijaloga **Ping sa**, unesite Sistem C u polje **Ping**.
4. Kliknite **Ping sada** da provjerite povezanost od Sistema A do Sistema C.
5. Kliknite **OK** pri završetku.

Scenarij: Zaštita L2TP dobrovoljnog tunela uz IPSec

U ovom scenariju, naučite kako postaviti vezu između hosta područnog ureda i korporativnog ureda koji koristi L2TP koji štiti IPSec. Područni ured ima dinamički dodijeljenu IP adresu, dok korporativni ured ima statičku, globalno usmjerljivu IP adresu.

Situacija

Pretpostavite da vaše poduzeće ima manji područni ured u drugoj županiji. U bilo koje radno vrijeme ured podružnice može zahtijevati pristup povjerljivim informacijama o System i modelu unutar vašeg korporativnog intraneta. Vaše poduzeće trenutno koristi skupe iznajmljene linije da omogući područnom uredu pristup na korporativnu mrežu. Iako vaše poduzeće želi nastaviti omogućavati siguran pristup vašem intranetu, vi odlučno želite smanjiti trošak koji za sobom nosi iznajmljena linija. To se može napraviti kreiranjem Sloj 2 Tunelskog protokola (L2TP) dobrovoljnog tunela koji proširuje vašu korporativnu mrežu, tako da se čini da je područni ured dio vaše korporativne podmreže. VPN štiti promet podataka preko L2TP tunela.

Pomoću L2TP dobrovoljnog tunela, udaljeni područni ured postavlja tunel direktno na L2TP mrežni poslužitelj (LNS) korporativne mreže. Funkcionalnost L2TP koncentratora pristupa (LAC) se nalazi na klijentu. Tunel je transparentan za Dobavljača Internet usluga (ISP) udaljenog klijenta, zato nije potrebno da ISP podržava L2TP. Ako želite više pročitati o L2TP konceptima, pogledajte Tunel protokol sloja 2 (L2TP).

Važno: Ovaj scenarij prikazuje sigurnosne gatewaye koji su direktno spojeni na Internet. Nepostojanje vatrozida je zbog jednostavnosti scenarija. To ne znači da upotreba vatrozida nije potrebna. Uzmite u obzir sigurnosne mjere svaki put kad se povezujete na Internet.

Ciljevi

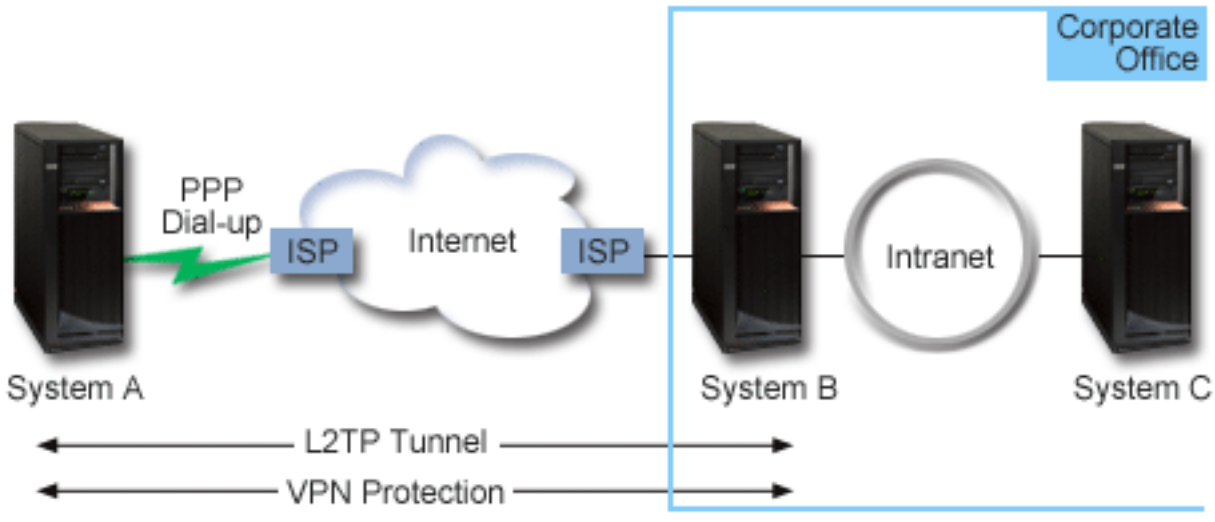
U ovom scenariju, sistem područnog ureda se spaja na korporativnu mrežu preko gateway sistema s L2TP tunelom koji štiti VPN.

Glavni ciljevi ovog scenarija su:

- Sistem područnog ureda uvijek započinje vezu s korporativnim uredom.
- Sistem područnog ureda je jedini sistem na mreži područnog ureda koji treba pristup na korporativnu mrežu. Drugim riječima, njegova uloga je uloga hosta, a ne prilaza, na mreži područnog ureda.
- Korporativni sistem je host računalo na mreži korporativnog ureda.

Detalji

Sljedeća slika ilustrira mrežne karakteristike za ovaj scenarij:



Sistem A

- Mora imati pristup TCP/IP aplikacijama na svim sistemima u korporativnoj mreži.

- Prima dinamički dodijeljene IP adrese od svog ISP-a.
- Mora biti konfiguriran da omogući L2TP podršku.

Sistem B

- Mora imati pristup TCP/IP aplikacijama na Sistemu A.
- Podmreža je 10.6.0.0 s maskom 255.255.0.0. Ova podmreža za podatke predstavlja krajnju točku VPN tunela na korporativnoj strani.
- Povezuje se na Internet s IP adresom 205.13.237.6. Ovo je krajnja točka veze. To znači da Sistem B izvodi upravljanje ključa i primjenjuje IPSec na dolazne i izlazne IP datograme. Sistem B se povezuje na svoju podmrežu s IP adresom 10.6.11.1.

U L2TP uvjetima, *Sistem A* radi kao L2TP inicijator, dok *Sistem B* radi kao L2TP završni dio programa.

Konfiguracijski zadaci

Pod pretpostavkom da TCP/IP konfiguracija već postoji i radi, morate dovršiti sljedeće zadatke:

Srodni koncepti

"Protokol tunela sloja 2" na stranici 7
Veze Protokola tunela sloja 2 (L2TP), koje su nazvane i virtualne linije, osiguravaju isplativiji pristup udaljenim korisnicima dopuštajući sistemima korporativne mreže da upravljaju IP adresama koje su dodijeljene njihovim udaljenim korisnicima. Nadalje, L2TP veze omogućuju siguran pristup vašem sistemu ili mreži kada ih koristite u spoju s protokolom IP sigurnosti (IPSec).

Srodne informacije

AS/400 Scenariji Internet sigurnosti: Praktični pristup, SG24-5954-00

Konfiguriranje VPN-a na Sistemu A

Dovršite sljedeće korake za konfiguriranje VPN veze na Sistemu A.

Koristite informacije iz vaših radnih tablica planiranja, da konfigurirate VPN na Sistemu A, kako slijedi:

1. **Konfigurirajte politiku Internet razmjene ključa**
   a. U System i Navigator, proširite Sistem A → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **IP politike sigurnosti**.
   b. Desno kliknite na **Politike razmjene Internet ključeva** i izaberite **Nova politika razmjene Internet ključeva**.
   c. Na stranici **Udaljeni poslužitelj** izaberite **Verzija 4 IP adresa** kao tip identifikatora i zatim upišite 205.13.237.6 u polje **IP adresa**.
   d. Na stranici **Asocijacije** izaberite **Unaprijed podijeljeni ključ** da označite da ova veza koristi unaprijed podijeljeni ključ za provjeru autentičnosti ove politike.
   e. Upišite unaprijed podijeljeni ključ u polje **Ključ**. Odnosite se prema svom dijeljenom ključu kao prema lozinci.
   f. Izaberite **Identifikator ključa** za tip identifikatora lokalnog poslužitelja ključa, a zatim upišite identifikator u polje **Identifikator**. Na primjer, ovojeidkljuca. Zapamtite da lokalni poslužitelj ključa ima dinamički dodijeljenu IP adresu koju je nemoguće unaprijed znati. Sistem B koristi ovaj identifikator da identificira Sistem A kada Sistem A započinje vezu.
   g. Na stranici **Pretvorbe**, kliknite **Dodavanje** da bi dodali pretvorbe koje Sistem A predlaže Sistemu B za zaštitu ključa i da bi specificirao da li IKE politika koristi zaštitu identiteta kod početka dogovaranja faze 1.
   h. Na stranici **Pretvorba IKE Politike** izaberite **Unaprijed podijeljeni ključ** za vašu metodu provjere autentičnosti, **SHA** za vaš algoritam raspršenja i **3DES-CBC** za vaš algoritam za šifriranje. Prihvatite default vrijednosti za Diffie-Hellman grupu i kasnije Istek IKE ključeva.
   i. Kliknite **OK** da se vratite na stranicu **Pretvorbe**.
   j. Izaberite **IKE agresivni način pregovaranja (bez zaštite identiteta).**

Bilješka: Ako koristite preddijeljene ključeve i agresivni mod pregovaranja u konfiguraciji, izaberite takve lozinke koje bi se teže otkrile u hakerskim napadima koji skeniraju rječnik. Također se preporučuje da periodički mijenjate vaše lozinke.

k. Kliknite **OK** da spremite vaše konfiguracije.

2. **Konfiguriranje politike podataka**
   a. S VPN sučelja, desno kliknite **Politike podataka** i izaberite **Nova politika podataka**
   b. Na stranici **Općenito** navedite ime politike podataka. Na primjer, l2tprudaljenikorisnik
   c. Otiđite na stranicu **Prijedlozi**. Prijedlog je kolekcija protokola koje inicijalni i odzivni poslužitelji ključeva koriste da uspostave dinamičku vezu između dvije krajnje točke. Pojedinu politiku podataka možete koristiti u nekoliko objekata veze. Međutim, nemaju nužno svi udaljeni VPN poslužitelji ključa ista svojstva politika podataka. Stoga, možete dodati nekoliko prijedloga jednoj politici podataka. Kod uspostave VPN veze na udaljeni poslužitelj ključa, mora biti najmanje jedan podudarajući prijedlog u politici podataka inicijatora i odzivnika.
   d. Kliknite **Dodaj** za dodavanje pretvorbe politike podataka
   e. Izaberite **Prijenos** za način sažimanja.
   f. Kliknite **OK** da se vratite na stranicu **Pretvorbe**.
   g. Navedite vrijednost za istek ključa.
   h. Kliknite **OK** da spremite vašu novu politiku podataka.
3. **Konfiguriranje grupe dinamičkog ključa**
   a. Iz VPN sučelja proširite **Sigurne veze**.
   b. Desno kliknite **Po grupi** i izaberite **Nova grupa dinamičkog ključa**.
   c. Na stranici **Općenito** navedite ime za grupu. Na primjer, l2tptocorp.
   d. Izaberite **Štiti lokalno inicirani L2TP tunel**.
   e. Za ulogu sistema izaberite **Oba sistema su hostovi**.
   f. Otiđite na stranicu **Politika**. Izaberite politiku podataka koju ste kreirali u koraku **Konfiguriranje politike podataka**, l2tpudaljenikorisnik, s popisa **Politike podataka**.
   g. Izaberite **Lokalni sistem započinje vezu**, da označite da samo Sistem A može započeti veze sa Sistemom B.
   h. Otiđite na stranicu **Veze**. Izaberite **Generiranje sljedećeg pravila filtriranja politike za ovu grupu**. Kliknite **Uredi** da definirate parametre filtera za politiku.
   i. Na stranici **Filter politike - Lokalne adrese** izaberite **Identifikator ključa** za tip identifikatora.
   j. Za identifikator izaberite identifikator ključa thisisthekeyid, koji ste definirali u IKE politici.
   k. Otiđite na stranicu **Filter politike - Udaljene adrese**. Izaberite **IP verzija 4 adresa** iz padajuće liste **Tip identifikatora**.
   l. Upišite 205.13.237.6 u polju **Identifikator**.
   m. Otiđite na stranicu **Filter politike - Servisi**. Upišite 1701 u poljima **Lokalni port** i **Udaljeni port**. Port 1701 je dobro poznati port za L2TP.
   n. Izaberite **UDP** iz padajuće liste **Protokol**.
   o. Kliknite **OK** da se vratite na stranicu **Veze**.
   p. Otiđite na stranicu **Sučelja**. Izaberite bilo koju liniju ili PPP profil na koji će se ova grupa primijeniti. Još niste kreirali PPP profil za ovu grupu. Nakon što to napravite, trebat ćete urediti svojstva ove grupe tako da se grupa primjenjuje na PPP profil koji kreirate u sljedećem koraku.
   q. Kliknite **OK** da kreirate grupu dinamičkog ključa, l2tptocorp.
4. **Konfiguriranje grupe dinamičke veze**
   a. Iz VPN sučelja proširite **Po grupi**. To prikazuje listu svih grupa dinamičkog ključa koje ste konfigurirali na Sistemu A.
   b. Desno kliknite na **l2tptocorp** i izaberite **Nova veza dinamičkog ključa**.
   c. Na stranici **Općenito** navedite opcijski opis za vezu.
   d. Za udaljeni poslužitelj ključa izaberite **Verzija 4 IP adresa** za tip identifikatora.

e. Izaberite 205.13.237.6 iz padajuće liste **IP adresa**.

f. Poništite izbor **Pokretanje na zahtjev**.

g. Otiđite na stranicu **Lokalne adrese**. Izaberite **Identifikator ključa** za tip identifikatora i zatim izaberite thisisthekeyid iz padajuće liste **Identifikator**.

h. Otiđite na stranicu **Udaljene adrese**. Izaberite **IP verzija 4 adresa** za tip identifikatora.

i. Upišite 205.13.237.6 u polju **Identifikator**.

j. Otiđite na stranicu **Usluge**. Upišite 1701 u poljima **Lokalni port** i **Udaljeni port**. Port 1701 je dobro poznati port za L2TP.

k. Izaberite **UDP** s popisa **Protokol**

l. Kliknite **OK** da kreirate vezu dinamičkog ključa.

Srodni zadaci

"Konfiguriranje VPN-a na Sistemu B" na stranici 26
Da konfigurirate VPN vezu na Sistemu B, slijedite iste korake koje ste koristili da konfigurirate VPN vezu na Sistemu A i promijenite IP adrese i identifikatore po potrebi.

Konfiguriranje profila PPP veze i virtualnog profila na Sistemu A

Sada kada je VPN veza konfigurirana na Sistemu A, trebate kreirati PPP profil za Sistem A. PPP profil nema pridruženu fizičku liniju; umjesto toga on koristi virtualnu liniju. To je zato što PPP promet tunelira kroz L2TP tunel, dok VPN štiti L2TP tunel.

Slijedite ove korake da kreirate profil PPP veze za Sistem A:

1. U System i Navigator, proširite Sistem A → **Mreža** → **Usluge udaljenog pristupa**.
2. Desno kliknite **Profili davaoca veze** i izaberite **Novi profil**.
3. Na stranici **Postav** izaberite **PPP** za tip protokola.
4. Za izbor Načina izaberite **L2TP (virtualna linija)**.
5. Izaberite **Inicijator na zahtjev (dobrovoljni tunel)** iz padajuće liste **Operacijski način**.
6. Kliknite **OK** da odete na stranicu svojstava PPP profila.
7. Na stranici **Općenito** upišite ime koje identificira tip i odredište veze. U ovom slučaju, upišite toCORP. Ime koje navedete mora imati 10 ili manje znakova.
8. Opcijski: Navedite opis profila.
9. Otiđite na stranicu **Veza**.
10. U polju **Ime virtualne linije** izaberite **tocorp** iz padajuće liste. Zapamtite da ova linija nema pridruženo fizičko sučelje. Virtualna linija opisuje različite karakteristike ovog PPP profila; na primjer, maksimalnu veličinu okvira, informacije o provjeri autentičnosti, ime hosta i tako dalje. Otvorit će se kućica dijaloga **Svojstva L2TP linije**.
11. Na stranici **Općenito** upišite opis za virtualnu liniju.
12. Otiđite na stranicu **Provjera autentičnosti**.
13. U polje **Ime lokalnog hosta** unesite ime hosta lokalnog ključnog poslužitelja, Sistem A.
14. Kliknite **OK** da spremite opis nove virtualne linije i vratite se na stranicu **Veza**.
15. Upišite adresu krajnje točke za udaljeni tunel, 205.13.237.6 u polju **Adresa krajnje točke za udaljeni tunel**.
16. Izaberite **Zahtijeva IPSec zaštitu** i izaberite grupu dinamičkog ključa koju ste kreirali u prethodnom koraku "Konfiguriranje VPN-a na Sistemu A" na stranici 23, l2tptocorp iz drop-down popisa **Ime grupe veze**.
17. Otiđite na stranicu **TCP/IP Postavke**.
18. U odlomku **Lokalna IP adresa** izaberite **Dodijeljena od udaljenog sistema**.
19. U odlomku **Udaljena IP adresa** izaberite **Koristi čvrste IP adrese**. Upišite 10.6.11.1, što je IP adresa udaljenog sistema na njegovoj podmreži.
20. U odlomku za usmjeravanje, izaberite **Definiraj dodatne statičke smjerove** i kliknite **Smjerovi**. Ako nema informacija usmjeravanja danih u PPP profilu, onda Sistem A može dohvatiti samo krajnju točku udaljenog tunela, ali ne bilo koji drugi sistem na 10.6.0.0 podmreži.
21. Kliknite **Dodaj** da dodate unos za statički smjer.

22. Upišite podmrežu, 10.6.0.0 i masku podmreže 255.255.0.0 da usmjerite sav 10.6.*.* promet kroz L2TP tunel.
23. Kliknite **OK** da dodate statički smjer.
24. Kliknite **OK** da zatvorite kućicu dijaloga Usmjeravanje.
25. Otiđite na stranicu **Provjera autentičnosti** da postavite korisničko ime i lozinku za ovaj PPP profil.
26. U odlomku za identifikaciju Lokalnog sistema, izaberite **Dozvoli udaljenom sistemu da provjeri identitet ovog sistema**.
27. Pod **Korištenja protokola provjere autentičnosti** izaberite **Zahtjev za šifriranom lozinkom (CHAP-MD5)**. U odjeljku identifikacije Lokalnog sistema, izaberite **Udaljenom sistemu omogući provjeru identiteta ovog sistema**.
28. Unesite korisničko ime Sistem A i lozinku.
29. Kliknite **OK** da spremite PPP profil.

Primjena l2tptocorp grupe dinamičkog ključa na toCorp PPP profil

Nakon što ste konfigurirali profil vaše PPP veze, trebate se vratiti natrag u grupu dinamičkog ključa l2tptocorp, koju ste kreirali i pridružili PPP profilu.

Da pridružite vašu grupu dinamičkog ključa vašem PPP profilu, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze → Po grupi**.
2. Desno kliknite grupu dinamičkog ključa, l2tptocorp i izaberite **Svojstva**.
3. Idite na stranicu **Sučelja** i izaberite **Primjena ove grupe** za PPP profil kreiran u “Konfiguriranje profila PPP veze i virtualnog profila na Sistemu A” na stranici 25, toCorp.
4. Kliknite **OK** da primijenite l2tptocorp na PPP profil, toCorp.

Konfiguriranje VPN-a na Sistemu B

Da konfigurirate VPN vezu na Sistemu B, slijedite iste korake koje ste koristili da konfigurirate VPN vezu na Sistemu A i promijenite IP adrese i identifikatore po potrebi.

Uzmite ove ostale točke u obzir prije nego započnete:

- Identificirajte udaljeni ključni poslužitelj identifikatorom ključa koji ste naveli za lokalni ključni poslužitelj na Sistemu A. Na primjer, thisisthekeyid.
- Koristite *točno* isti unaprijed podijeljeni ključ.
- Osigurajte da vaše pretvorbe odgovaraju onima koje ste konfigurirali na Sistemu A ili veze neće uspjeti.
- Ne navodite **Štiti lokalno inicirani L2TP tunel** na stranici **Općenito** grupe dinamičkog ključa.
- Udaljeni sistem započinje vezu.
- Navedite da se veza treba pokrenuti na zahtjev.

Srodni zadaci

“Konfiguriranje VPN-a na Sistemu A” na stranici 23
Dovršite sljedeće korake za konfiguriranje VPN veze na Sistemu A.

Konfiguriranje profila PPP veze i virtualne linije na Sistemu B

Sada kada je VPN veza konfigurirana na Sistemu B, trebate kreirati PPP profil za Sistem B. PPP profil nema pridruženu fizičku liniju: umjesto toga koristi virtualnu liniju. To je zato što PPP promet tunelira kroz L2TP tunel, dok VPN štiti L2TP tunel.

Slijedite ove korake da kreirate profil PPP veze za System B:

1. U System i Navigator, proširite Sistem B → **Mreža → Usluge udaljenog pristupa**.
2. Desno kliknite **Profili odzivnika veze** i izaberite **Novi profil**.
3. Na stranici **Postav** izaberite **PPP** za tip protokola.
4. Za izbor Načina izaberite **L2TP (virtualna linija)**.

5. Izaberite **Terminator (mrežni poslužitelj)** iz padajuće liste **Način rada**.
6. Kliknite **OK** na stranicama svojstava PPP profila.
7. Na stranici **Općenito** upišite ime koje identificira tip i odredište veze. U ovom slučaju, upišite tobranch. Ime koje navedete mora imati 10 ili manje znakova.
8. Opcijski: Navedite opis profila.
9. Otiđite na stranicu **Veza**.
10. Izaberite IP adresu krajnje točke lokalnog tunela, 205.13.237.6.
11. U polju **Ime virtualne linije** izaberite **tobranch** iz padajuće liste. Zapamtite da ova linija nema pridruženo fizičko sučelje. Virtualna linija opisuje različite karakteristike ovog PPP profila; na primjer, maksimalnu veličinu okvira, informacije o provjeri autentičnosti, ime hosta i tako dalje. Otvorit će se kućica dijaloga **Svojstva L2TP linije**.
12. Na stranici **Općenito** upišite opis za virtualnu liniju.
13. Idite na stranicu **Provjera autentičnosti**
14. U polje **Ime lokalnog hosta** unesite ime hosta lokalnog ključnog poslužitelja SystemB.
15. Kliknite **OK** da spremite opis nove virtualne linije i vratite se na stranicu **Veza**.
16. Otiđite na stranicu **TCP/IP Postavke**.
17. U odlomku **Lokalna IP adresa**, izaberite čvrstu IP adresu lokalnog sistema, 10.6.11.1.
18. U odlomku **Udaljena IP adresa** izaberite **Spremište adresa** kao metodu dodjele adresa. Upišite početnu adresu, a zatim navedite broj adresa koje mogu biti dodijeljene udaljenom sistemu.
19. Izaberite **Dozvoli udaljenom sistemu pristup drugim mrežama (IP prosljeđivanje)**.
20. Otiđite na stranicu **Provjera autentičnosti** da postavite korisničko ime i lozinku za ovaj PPP profil.
21. U odlomku za identifikaciju Lokalnog sistema, izaberite **Dozvoli udaljenom sistemu da provjeri identitet ovog sistema**. Ovo otvara kućicu dijaloga **Identifikacija Lokalnog Sistema**.
22. Pod **Korištenje protokola provjere autentičnosti** izaberite **Zahtjev za šifriranom lozinkom (CHAP-MD5)**.
23. Unesite korisničko ime, Sistem B i lozinku.
24. Kliknite **OK** da spremite PPP profil.

Aktiviranje paketnih pravila

VPN čarobnjak automatski kreira paketna pravila koje ova veza zahtijeva za ispravan rad. Međutim, njih morate aktivirati na oba sistema prije nego možete pokrenuti VPN vezu.

Da aktivirate paketna pravila na Sistemu A, slijedite ove korake:

1. U System i Navigator, proširite **Sistem A → Mreža → IP Politike**.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje paketnih pravila**.
3. Izaberite želite li aktivirati samo VPN generirana pravila, samo izabranu datoteku ili oboje, VPN generirana pravila i izabranu datoteku. Ovo posljednje biste mogli izabrati ako, na primjer, imate svakovrsna PERMIT i DENY pravila koja želite nametnuti sučelju kao dodatak VPN generiranim pravilima.
4. Izaberite sučelje na kojem želite aktivaciju pravila. U ovom slučaju, izaberite **Sva sučelja**.
5. Kliknite na **OK** u kućici dijaloga da potvrdite kako želite provjeriti i aktivirati pravila na sučelju ili sučeljima koje ste naveli. Nakon što kliknete OK, sistem provjerava pravila od sintaktičkih i semantičkih pogrešaka i daje izvještaj o rezultatima u prozoru za poruke na dnu editora. Za poruke o greškama koje se odnose na određenu datoteku ili broj linije, možete desno kliknuti na grešku i izabrati **Idi na liniju** da osvijetlite grešku u datoteci.
6. Da aktivirate paketna pravila na Sistemu B, ponovite ove korake.

Scenarij: VPN naklonjen vatrozidu

U ovom scenariju, veliko osiguravajuće poduzeće želi uspostaviti VPN između gatewaya u Chicagu i hosta u Minneapolisu, a obje mreže su iza vatrozida.

Situacija

Pretpostavite da ste veliko osiguravajuće poduzeće iz Minneapolisa i upravo ste otvorili podružnicu u Chicagu. Podružnica u Chicagu želi pristupiti bazi podataka korisnika iz stožera u Minneapolisu. Želite biti sigurni da su informacije koje prenosite sigurne, jer baza podataka sadrži povjerljive informacije o korisnicima, kao što su imena, adrese i brojevi telefona. Odlučili ste povezati obje podružnice preko Interneta korištenjem virtualne privatne mreže (VPN). Obje podružnice su iza vatrozida i koriste prijevod mrežne adrese (NAT) da sakriju svoju neregistriranu privatnu IP adresu iza skupa registriranih IP adresa. Međutim, postoji nekompatibilnost VPN veza s NAT. VPN veza odbacuje pakete koji su poslani preko NAT uređaja, jer NAT mijenja IP adresu u paketu, čineći ga nevažećim. Međutim i dalje možete koristiti VPN vezu s NAT ako primijenite UDP sažimanje.

U ovom scenariju, privatna IP adresa iz Chicago mreže je stavljena u novi IP naslov i dohvaća prijevod kada ide kroz vatrozid C (pogledajte sljedeću sliku). Onda, kada paket dosegne vatrozid D, on će prevesti IP adresu odredišta u IP adresu Sistema E, nadalje će se paket proslijediti do Sistema E. Na kraju, kada paket dosegne Sistem E, on isključuje UDP naslov i ostavlja originalni IPSec paket, koji će sada proći sve provjere valjanosti o dozvoliti sigurnu VPN vezu.

Ciljevi

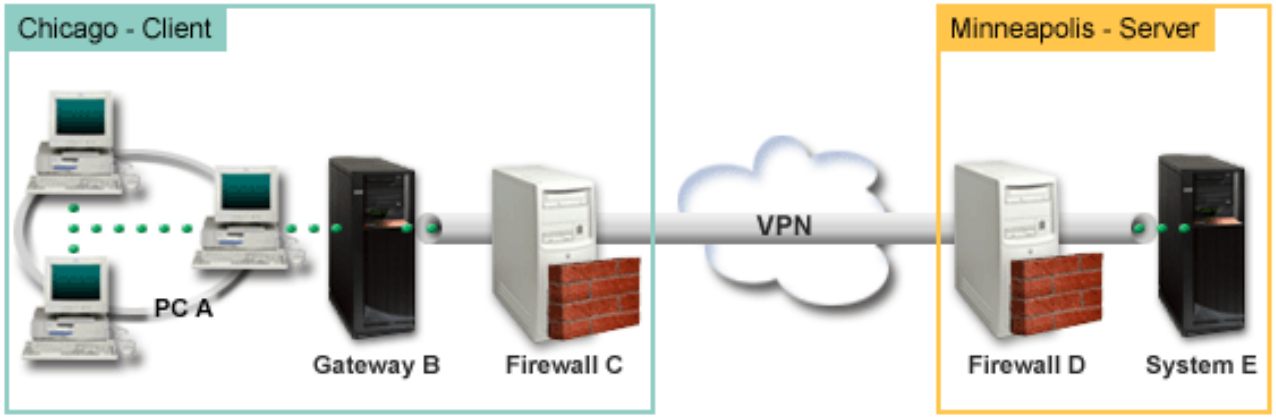
U ovom scenariju, veliko osiguravajuće poduzeće želi uspostaviti VPN između gatewaya u Chicagu (klijent) i hosta u Minneapolisu (poslužitelj), a obje mreže su iza vatrozida.

Ciljevi ovog scenarija su sljedeći:

- Gateway podružnice u Chicagu uvijek započinje vezu s hostom u Minneapolisu.
- VPN mora štititi sav promet podataka između gatewaya u Chicagu i hosta u Minneapolisu.
- Dozvolite korisnicima u Chicago prilazu pristup do System i baze podataka koja je smještena u Minneapolis mreži preko VPN veze.

Detalji

Sljedeća slika ilustrira mrežne karakteristike za ovaj scenarij:



Chicago mreža - klijent

- Prilaz B se izvodi nai5/OS verziji 5 Izdanju 4 (V5R4) ili kasnijem.
- Prilaz B se povezuje na Internet s IP adresom 214.72.189.35 i krajnja je točka veze VPN tunela. Prilaz B obavlja IKE dogovaranja i primjenjuje UDP sažimanje na izlazne IP datograme.
- Prilaz B i PC A su u podmreži 10.8.11.0 s maskom 255.255.255.0
- PC A je izvorno odredište za podatke koji teku preko VPN veze, nadalje, on je krajnja točka podataka VPN tunela.
- Samo Prilaz B može započeti vezu sa Sistemom E.

- Vatrozid C ima Masq NAT pravilo s javnom IP adresom 129.42.105.17 koja skriva IP adresu Prilaza B

Minneapolis mreža - Poslužitelj

- Sistem E se izvodi na i5/OS verziji 5 izdanju 4 (V5R4) ili kasnijem.
- Sistem E ima IP adresu 56.172.1.1.
- Sistem E je odgovaratelj na zahtjev, za ovaj scenarij.
- Vatrozid D ima i IP adresu 146.210.18.51.
- Vatrozid D ima Statičko NAT pravilo koje mapira javni IP (146.210.18.15) na privatni IP Sistema E (56.172.1.1). Nadalje, od klijentove perspektivne IP adrese Sistema E, javna IP adresa je (146.210.18.51) vatrozida D.

Zadaci konfiguracije

Srodni koncepti

"Upravljanje ključevima" na stranici 6
Dinamički VPN daje dodatnu sigurnost za vaše komunikacije korištenjem protokola Internet razmjena ključa (IKE) za upravljanje ključem. IKE dozvoljava VPN poslužiteljima na svakom kraju veze da pregovaraju nove ključeve u određenim intervalima.

"NAT kompatibilni IPSec s UDP" na stranici 9
UDP dozvoljava IPSec prometu da prođe kroz konvencionalan NAT uređaj. Pregledajte ovo poglavlje za više informacija o tome što je to i zašto bi ga koristili za vaše VPN veze.

Dovršenje radne tablice planiranja

Sljedeća kontrolna lista za planiranje ilustrira tip informacija koje trebate prije nego započnete konfiguriranje VPN-a. Svi odgovori na preduvjetnoj kontrolnoj listi moraju biti DA prije nego nastavite s postavljanjem VPN-a.

Bilješka: Dvije su odijeljene radne tablice za Prilaz B i Sistem E.

Tablica 5. Sistemski zahtjevi

Kontrolna lista preduvjeta	**Odgovori**
Je li vaš operativni sistem i5/OS V5R4 ili kasniji?	Da
Je li Upravitelj digitalnih certifikata opcija instalirana?	Da
Da li je instaliran System i Access za Windows?	Da
Da li je instaliran System i Navigator?	Da
Da li je instalirana mrežna pomoćna komponenta System i Navigator ?	Da
Da li je instaliran IBM TCP/IP pomoćni programi povezanosti za i5/OS?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na sistemu (uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene)?	Da
Da li je uspostavljena normalna TCP/IP komunikacija između zahtijevanih krajnjih točaka?	Da
Jeste li primijenili privremene popravke za posljednji program (PTF-ove)?	Da
Ako VPN tunel prolazi kroz vatrozid ili usmjerivače koji koriste IP filtriranje, da li pravila filtriranja vatrozida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatrozidovi ili usmjerivači konfigurirani za dozvolu prometa preko porta 4500 za pregovore o ključu. Tipično, VPN partneri obavljaju IKE pregovore preko UDP porta 500, a kad IKE detektira NAT pakete, šalju se preko porta 4500.	Da
Da li su vatrozidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Tablica 6. Konfiguracija Prilaza B

Trebate ove informacije za konfiguriranje VPN-a za Prilaz B	**Odgovori**
Koji tip veze kreirate?	gateway-do-drugog hosta
Kako ćete nazvati grupu dinamičkog ključa?	CHIgw2MINhost
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših ključeva?	uravnoteženi
Da li koristite certifikate za provjeru autentičnosti veze? Ako ne, koji je unaprijed podijeljeni ključ?	Ne : topsecretstuff
Koji je identifikator za lokalnog poslužitelja ključa?	IP adresa: 214.72.189.35
Koji je identifikator za lokalnu krajnju točku podataka?	Podmreža: 10.8.11.0 Maska: 255.255.255.0
Koji je identifikator udaljenog poslužitelja ključa?	IP adresa: 146.210.18.51
Koji je identifikator za udaljenu krajnju točku podataka?	IP adresa: 146.210.18.51
Koje portove i protokole želite dozvoliti za protok vezom?	Bilo koje
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka?	uravnoteženi
Na koja se sučelja veza odnosi?	TRLINE

Tablica 7. Konfiguracija Sistema E

Trebate ove informacije za konfiguriranje VPN-a za Sistem E	**Odgovori**
Koji tip veze kreirate?	host-do-drugog gatewaya
Kako ćete nazvati grupu dinamičkog ključa?	CHIgw2MINhost
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših ključeva?	najviši
Da li koristite certifikate za provjeru autentičnosti veze? Ako ne, koji je unaprijed podijeljeni ključ?	Ne : topsecretstuff
Koji je identifikator za lokalnog poslužitelja ključa?	IP adresa: 56.172.1.1
Koji je identifikator udaljenog poslužitelja ključeva? **Bilješka:** Ako je IP adresa vatrozida C nepoznata, možete koristiti *ANYIP kao identifikator za udaljeni ključni poslužitelj.	IP adresa: 129.42.105.17
Koji je identifikator za udaljenu krajnju točku podataka?	Podmreža: 10.8.11.0 Maska: 255.255.255.0
Koje portove i protokole želite dozvoliti za protok vezom?	Bilo koje
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka?	najviši
Na koja se sučelja veza odnosi?	TRLINE

Srodne reference

Savjetnik za planiranje VPN-a

Konfiguriranje VPN-a na Prilazu B

Dovršite sljedeće korake da konfigurirate VPN vezu na Prilazu B.

Koristite informacije iz vaših radnih tablica planiranja, da konfigurirate VPN na Prilazu B kako slijedi:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete Čarobnjaka za vezu.
3. Pregledajte stranicu **Pozdrav** za informacije o objektima koje kreira čarobnjak.
4. Kliknite **Sljedeće** za odlazak na stranicu **Ime veze**
5. U polje **Ime** unesite CHIgw2MINhost.
6. Opcijski: Navedite opis ove grupe veza.
7. Kliknite **Sljedeće** za odlazak na stranicu **Scenario veze**.
8. Izaberite **Povežite vaš gateway na drugi host**.

9. Kliknite **Sljedeće** za odlazak na stranicu **Politika razmjene Internet ključeva.**
10. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.

    Bilješka: Ako dobijete poruku greške ″Zahtjev za certifikatom se ne može obraditi″, možete ga ignorirati jer ne koristite certifikate za razmjenu ključa.
11. Opcijski: Ako imate certifikate instalirane, vidjet ćete stranicu **Certifikat za krajnju točku Lokalne veze**. Izaberite Ne da označite da nećete koristiti certifikate za provjeru autentičnosti veze.
12. Kliknite **Sljedeće** da odete na stranicu **Lokalni poslužitelj ključeva**.
13. Izaberite **IP verzija 4 adresa** iz polja **Tip identifikatora**.
14. Izaberite 214.72.189.35 iz polja **IP adresa**.
15. Kliknite **Sljedeće** za odlazak na stranicu **Udaljeni poslužitelj s ključevima**.
16. Izaberite **IP verzija 4 adresa** u polju **Tip identifikatora**.
17. Upišite 146.210.18.51 u polju **Identifikator**.

    Bilješka: Gateway B započinje vezu sa Static NAT i morate navesti glavni način razmjene ključa da bi unijeli pojedinačni IP za udaljeni ključ. Glavni način razmjene ključa po defaultu je izabran pri kreiranju veze s VPN čarobnjakom veze. Ako se u ovoj situaciji koristi agresivni način, za udaljeni ključ mora se unijeti udaljeni identifikator tipa koji nije IPV4.
18. Unesite topsecretstuff u polju **Preddijeljeni ključ**
19. Kliknite na **Sljedeće** da odete na stranicu **Lokalna krajnja točka podataka**.
20. Izaberite **IP verzija 4 podmreža** iz polja **Tip identifikatora**.
21. Upišite 10.8.0.0 u polju **Identifikator**.
22. Upišite 255.255.255.0 u polju **Maska podmreže**.
23. Kliknite na **Sljedeće** da odete na stranicu **Usluge podataka**.
24. Prihvatite defaultne vrijednosti i kliknite na **Sljedeće** za odlazak na stranicu Politike podataka.
25. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.
26. Kliknite **Sljedeće** za odlazak na stranicu **Primjenjiva sučelja.**
27. Izaberite **TRLINE** iz tablice linija.
28. Kliknite **Sljedeće** za odlazak na stranicu **Sažetak.**
29. Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.
30. Kliknite **Završetak** za dovršetak konfiguracije.
31. Kad se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Da**, aktiviraj generirane filtere politike, tada izaberite **Dozvoli sav ostali promet**.
32. Kliknite **OK** da dovršite konfiguraciju.

Konfiguriranje VPN-a na Sistemu E

Dovršite sljedeće korake za konfiguriranje VPN veze na Sistemu E.

Koristite informacije iz vaših radnih tablica planiranja, da konfigurirate VPN na Sistemu E kako slijedi:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete Čarobnjaka za vezu.
3. Pregledajte stranicu **Pozdrav** za informacije o objektima koje kreira čarobnjak.
4. Kliknite **Sljedeće** za odlazak na stranicu **Ime veze**
5. U polje **Ime** unesite CHIgw2MINhost.
6. Opcijski: Navedite opis ove grupe veza.
7. Kliknite **Sljedeće** za odlazak na stranicu **Scenario veze**.
8. Izaberite **Povežite vaš prilaz na drugi prilaz**.
9. Kliknite **Sljedeće** za odlazak na stranicu **Politika razmjene Internet ključeva.**

10. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.

    Bilješka: Ako dobijete poruku greške ″Zahtjev za certifikatom se ne može obraditi″, možete ga ignorirati jer ne koristite certifikate za razmjenu ključa.
11. Opcijski: Ako imate certifikate instalirane, vidjet ćete stranicu **Certifikat za krajnju točku Lokalne veze**. Izaberite Ne da označite da nećete koristiti certifikate za provjeru autentičnosti veze.
12. Kliknite **Sljedeće** da odete na stranicu **Lokalni poslužitelj ključeva**.
13. Izaberite **IP verzija 4 adresa** iz polja **Tip identifikatora**.
14. Izaberite 56.172.1.1 iz polja **IP adresa**.
15. Kliknite **Sljedeće** za odlazak na stranicu **Udaljeni poslužitelj s ključevima**.
16. Izaberite **IP verzija 4 adresa** u polju **Tip identifikatora**.
17. Upišite 129.42.105.17 u polju **Identifikator**.

    Bilješka: Ako je IP adresa vatrozida C nepoznata, možete koristiti *ANYIP kao identifikator za udaljeni ključni poslužitelj.
18. Unesite topsecretstuff u polju **Preddijeljeni ključ**
19. Kliknite na **Sljedeće** da odete na stranicu **Udaljena krajnja točka podataka**.
20. Izaberite **IP verzija 4 podmreža** iz polja **Tip identifikatora**.
21. Upišite 10.8.11.0 u polju **Identifikator**.
22. Upišite 255.255.255.0 u polju **Maska podmreže**.
23. Kliknite na **Sljedeće** da odete na stranicu **Usluge podataka**.
24. Prihvatite defaultne vrijednosti i kliknite na **Sljedeće** za odlazak na stranicu Politike podataka.
25. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.
26. Kliknite **Sljedeće** za odlazak na stranicu **Primjenjiva sučelja.**
27. Izaberite **TRLINE** iz tablice linija.
28. Kliknite **Sljedeće** za odlazak na stranicu **Sažetak.**
29. Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.
30. Kliknite **Završetak** za dovršetak konfiguracije.
31. Kad se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Da**, aktiviraj generirane filtere politike, tada izaberite **Dozvoli sav ostali promet**.
32. Kliknite **OK** da dovršite konfiguraciju.

Pokretanje veze

Nakon konfiguracije vaše VPN veze na Sistemu E, trebate pokrenuti vašu VPN vezu.

Slijedite ove korake da potvrdite da je CHIgw2MINhost veza na Sistemu E aktivna:

1. U System i Navigator, proširite **Sistem E → Mreža → Sigurne veze → Sve veze**.
2. Pogledajte **CHIgw2MINhost** i provjerite da je polje **Status** *U mirovanju* ili *Na-zahtjev*.

Slijedite ove korake za pokretanje CHIgw2MINhost veze s Prilaza B:

1. U System i Navigator, proširite **Prilaz B → Mreža → IP politike**.
2. Ako VPN poslužitelj nije pokrenut, desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Pokreni**.
3. Proširite **Virtualno privatno umrežavanje → Sigurne veze**.
4. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
5. Desno kliknite **CHIgw2MINhost** i izaberite **Pokreni**.
6. Iz izbornika **Pogled** izaberite **Osvježi**. Ako se veza uspješno pokrene, polje **Status** promijenit će se od *Pokreće se* ili *Na-zahtjev* na *Omogućen*. Pokretanje povezivanja može potrajati nekoliko trenutaka, pa povremeno napravite osvježavanje dok se status ne promijeni u *Omogućeno*.

Testiranje veze

Nakon dovršenja konfiguracije za Prilaz B i Sistem E i uspješno pokrenutih VPN poslužitelja, testirajte povezanost da osigurate da oba sistema mogu komunicirati jedan s drugim.

Da testirate vaše veze, slijedite ove korake:

1. Nađite sistem na A mreži PC-a i otvorite Telnet sesiju.
2. Navedite javnu IP adresu za Sistem E, koja je 146.210.18.51.
3. Navedite informacije o loginu ako je potrebno. Ako možete gledati ekran prijave, veza radi.

Scenarij: VPN veza do udaljenih korisnika

Administrator treba konfigurirati vezu virtualne privatne mreže (VPN) do udaljenih korisnika da omogući udaljene veze.

Sljedeći zadaci vam pokazuju kako administrator konfigurira VPN vezu do udaljenih korisnika.

Dovršenje radnih tablica planiranja za VPN vezu iz ureda podružnice do udaljenih prodavača

Administrator za ured prodavača podružnice koristi VPN savjetnika planiranja, za kreiranje radnih tablica dinamičkog planiranja, da bi im pomogle u konfiguriranju virtualne privatne mreže (VPN) na njihovim sistemima i udaljenim radnim stanicama.

VPN savjetnik planiranja je interaktivni alat koji postavlja specifična pitanja koja se odnose na vaše VPN potrebe. Na temelju vaših odgovora, savjetnik generira prilagođenu radnu tablicu planiranja za vašu okolinu koja se može koristiti kada konfigurirate vašu VPN vezu. Ova radna tablica se onda može koristiti kada konfigurirate VPN na vašem sistemu. Svaka od sljedećih radnih tablica planiranja su generirane s VPN savjetnikom planiranja i korištene za konfiguriranje VPN-a, preko VPN Čarobnjaka nove veze u System i Navigator.

Tablica 8. Radna tablica planiranja VPN veze između prodajnog ureda podružnice i udaljenih prodavača

Što VPN čarobnjak pita	**Što VPN savjetnik preporučuje**
Kako biste nazvali ovu grupu povezivanja?	SalestoRemote
Koji tip grupe povezivanja želite kreirati?	Izaberite **Spojite vaš host na drugi host**
Koju Internet politiku razmjene ključa želite koristiti da bi zaštitili svoj ključ?	Izaberite **Kreiranje nove politike** i onda izaberite **najviša sigurnost, najlošija izvedba**
Koristite li certifikate?	Izaberite **Ne**
Unesite identifikator da prikažete poslužitelj lokalnog ključa za ovu vezu.	Tip identifikatora: **IP verzija 4 adrese**, IP adresa:**192.168.1.2**. Za IPv6 adresu, tip identifikatora: **IP verzija 6 adrese**, IP adresa:**2001:DB8::2** **Bilješka:** IP adrese korištene u ovom scenariju su samo u svrhu primjera. One ne odražavaju shemu IP adresiranja i ne bi se trebale koristiti ni u jednoj stvarnoj konfiguraciji. Kod dovršavanja ovih zadataka trebate koristiti vlastite IP adrese.

Tablica 8. Radna tablica planiranja VPN veze između prodajnog ureda podružnice i udaljenih prodavača (nastavak)

Što VPN čarobnjak pita	Što VPN savjetnik preporučuje
Koji je identifikator ključnog poslužitelja na koji se želite spojiti?	Tip identifikatora: **Bilo koja IP adresa**, **preddijeljeni ključ**: mycokey. **Bilješka:** Preddijeljeni ključ je 32-znakovni tekstualni niz koji i5/OS VPN koristi za provjeru autentičnosti kao i za postavljanje ključeva koji štite vaše podatke. Općenito bi trebali postupati s preddijeljenim ključem na isti način kao što postupate s lozinkom.
Koji su portovi i protokoli podataka koje će ova veza zaštititi?	**Lokalni port**: 1701, **Udaljeni port**: Bilo koji port, **Protokol**: UDP
Koju politiku podataka želite koristiti da zaštitite podatke?	Izaberite **Kreiranje nove politike** i onda izaberite **najviša sigurnost, najlošija izvedba**
Provjerite sučelja na lokalnom sistemu na koje će se ova veza primijeniti.	ETHLINE (ured prodavača podružnice)

Konfiguriranje profila L2TP terminatora za Sistem A

Ako želite konfigurirati udaljene veze na udaljene radne stanice, trebate postaviti Sistem A da prihvati ulazne veze s ovih klijenata.

Da konfigurirate Layer Two Tunneling Protocol (L2TP) profil terminatora za Sistem A, dovršite sljedeće korake:

1. Iz System i Navigator, proširite ***Sistem A*** → **Mreža** → **Usluge udaljenog pristupa**.
2. Desno-kliknite na **Profili veze primatelja** da postavite Sistem A kao poslužitelj koji dopušta dolazne veze od udaljenih korisnika i izaberite **Novi profil**.
3. Izaberite sljedeće opcije na stranici Postav:
   - **Tip protokola:** PPP
   - **Tip veze:** L2TP (virtualna linija)

     Bilješka: Polje **Način rada** bi trebalo automatski prikazati **Terminator (mrežni poslužitelj)**.
   - **Tip linije servisa:** jedna linija
4. Kliknite na **OK**. Ovo će lansirati stranicu Nova point-to-point svojstva profila.
5. Na kartici **Općenito** ispunite sljedeća polja:
   - **Ime**: MYCOL2TP
   - Izaberite **Pokretanje profila uz TCP**, ako želite da se profil automatski pokrene uz TCP.
6. Na kartici **Povezivanje**, izaberite **192.168.1.2** (**2001:DB8::2** u IPv6) za **IP adresu krajnje točke lokalnog tunela**.

   Važno: IP adrese korištene u ovom scenariju su samo u svrhu primjera. One ne odražavaju shemu IP adresiranja i ne bi se trebale koristiti ni u jednoj stvarnoj konfiguraciji. Koristite vlastite IP adrese kod dovršenja ovih zadataka.
7. Izaberite **MYCOL2TP** kao **Naziv virtualne linije**. Ovo će lansirati New L2TP Properties stranicu.
8. Na stranicu provjere autentičnosti unesite systema kao ime hosta. Kliknite na **OK**. To će vas vratiti na stranicu Povezivanje.
9. Na stranici Povezivanje, izaberite sljedeće opcije i unesite 25 kao **Maksimalan broj veza**.

a. Kliknite karticu **Provjera autentičnosti** i izaberite **Zahtijevanje ovog sistema za provjeru identiteta udaljenog sistema**.
b. Izaberite **Lokalna provjera s validacijskom listom**.
c. Unesite QL2TP u polje **Ime validacijske liste** i kliknite na **New**.

10. Na stranici Validacijska lista, izaberite **Dodavanje**.
11. Dodajte korisnička imena i lozinke za svakog udaljenog zaposlenika. Kliknite na **OK**.
12. Na stranici Potvrda lozinke, ponovno unesite lozinku za svakog udaljenog zaposlenika. Kliknite **OK**.
13. Na stranici TCP/IP postavljanja, izaberite 10.1.1.1 (2001:DA8::1 u IPv6) za **Lokalnu IP adresu**.
14. U polju **Način dodjele IP adrese**, izaberite **Spremište adrese**.
15. U polje **Pokretanje IP adrese**, unesite 10.1.1.100 i 49 za **Broj adresa**. Za IPv6 adresu, u polje **Pokretanje IP adrese**, unesite 2001:DA8::1:1 i 65535 za **Broj adresa**.
16. Izaberite **Dozvoli udaljenom sistemu pristup drugim mrežama (IP prosljeđivanje)**. Kliknite **OK**.

Pokretanje profila veze primatelja

Nakon konfiguriranja Layer Two Tunneling Protocol (L2TP) primatelja veze profila za Sistem A, administrator treba pokrenuti ovu vezu, pa će ona osluškivati dolazne zahtjeve s udaljenih klijenata.

Bilješka: Možda ćete primiti poruku greške koju QUSRWRK podsistem nije pokrenuo. Ova poruka se pojavi kod pokušaja pokretanja profila veze primatelja. Za pokretanje QUSRWRK podsistema, dovršite ove korake:

1. U sučelje bazirano na znakovima, unesite strsbs.
2. Na ekranu Pokretanje podsistema, unesite QUSRWRK u polje **Opis podsistema**.

Da pokrenete profil veze primatelja za udaljene klijente, dovršite ove zadatke:

1. U System i Navigator, izaberite **Osvježi** iz izbornika **Pogled**. Ovo će osvježiti vašu instancu System i Navigator.
2. U System i Navigator, proširite ***Sistem A*** → **Mreža** → **Usluge udaljenog pristupa**.
3. Dvostruko kliknite na **Profili veze primatelja** i desno-kliknite **MYCOL2TP** i izaberite **Pokretanje**.
4. Polje **Status** će prikazati **Čekanje zahtjeva za povezivanje**.

Konfiguriranje VPN veze na Sistemu A za udaljene klijente

Nakon konfiguriranja i pokretanja Layer Two Tunneling Protocol (L2TP) primatelja profila veze za Sistem A, administrator treba konfigurirati virtualnu privatnu mrežu (VPN) da zaštiti vezu između udaljenih klijenata i mreže u uredu prodavača podružnice.

Da konfigurirate VPN za udaljene klijente, dovršite ove korake:

Važno: IP adrese korištene u ovom scenariju su samo u svrhu primjera. One ne odražavaju shemu IP adresiranja i ne bi se trebale koristiti ni u jednoj stvarnoj konfiguraciji. Koristite vlastite IP adrese kod dovršenja ovih zadataka.

1. Iz System i Navigator, proširite ***Sistem A*** → **Mreža** → **IP politike**.
2. Desno-kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete VPN Čarobnjaka nove veze. Pregledajte stranicu dobrodošlice za informacije koje objekte čarobnjak kreira.
3. Kliknite **sljedeće** da odete na stranicu Ime veze.
4. U polje **Ime** upišite SalestoRemote.
5. Opcijsko: Navedite opis za ovu grupu veze. Kliknite **Sljedeće**.
6. Na stranici Scenarij veze, izaberite **Spojite vaš host na drugi host**. Kliknite **Sljedeće**
7. Na Internet stranici politike razmjene ključa, izaberite **Kreiranje nove politike** i onda izaberite **Najviša sigurnost, najlošija izvedba**. Kliknite **Sljedeće**.
8. Na stranici Certifikat za krajnju točku lokalne veze, izaberite **Ne**. Kliknite **Sljedeće**.
9. Na stranici Lokalni ključni poslužitelj, izaberite **Verzija 4 IP adrese** kao tip identifikatora. Pridružena IP adresa treba biti 192.168.1.2. Kliknite **Sljedeće**. Za IPv6 adresu, na stranici Lokalni ključni poslužitelj, izaberite **Verzija 6 IP adrese** kao tip identifikatora. Pridružena IP adresa bi trebala biti 2001:DB8::2. Kliknite **Sljedeće**.

10. Na stranici Udaljeni ključni poslužitelj, izaberite **Bilo koja IP adresa** u polju **Tip identifikatora**. U polje **Preddijeljeni ključ** unesite mycokey. Kliknite **Sljedeće**.
11. Na stranicu Usluge podataka, unesite 1701 za lokalni port. Onda izaberite 1701 za udaljeni port i izaberite **UDP** za protokol. Kliknite **Sljedeće**.
12. Na stranici Politika podataka, izaberite **Kreiranje nove politike** i onda izaberite **Najviša sigurnost, najniža izvedba**. Kliknite **Sljedeće**.
13. Na stranici Primjenjiva sučelja, izaberite **ETHLINE**. Kliknite **Sljedeće**.
14. Na stranici Sažetak, pregledajte objekte koje će čarobnjak kreirati da budete sigurni u njihovu ispravnost.
15. Kliknite **Završetak** za dovršetak konfiguracije. Kada se otvori prozor Aktiviranje filtera politike, izaberite **Kasnije se paketna pravila neće aktivirati**. Kliknite **OK**.

Ažuriranje VPN politika za udaljene veze s Windows XP i Windows 2000 klijenata

Budući da čarobnjak kreira standardnu vezu koja se može koristiti za većinu konfiguracija virtualne privatne mreže (VPN), trebat ćete ažurirati politike koje je čarobnjak generirao, da osigurate međuoperabilnost s Windows XP i Windows 2000 klijentima.

Da ažurirate ove VPN politike, dovršite sljedeće zadatke:

1. Iz System i Navigator, proširite ***Sistem A*** → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **IP Sigurnosne politike**.
2. Dvostruko kliknite na **Politike Internet razmjene ključa** i desno-kliknite na **Bilo koja IP adresa** i izaberite **Svojstva**.
3. Na stranici Pretvorbe, kliknite **Dodavanje**.
4. Na stranici Dodavanje stranice pretvorbe Internet razmjene ključa, izaberite sljedeće opcije:
   - **Način provjere autentičnosti:** Preddijeljeni ključ
   - **Algoritam raspršivanja:** MD5
   - **Algoritam šifriranja:** DES-CBC
   - **Diffie-Hellman grupa:** Grupa 1
5. Kliknite **OK**.
6. Iz System i Navigator, proširite ***Sistem A*** → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **IP Sigurnosne politike**.
7. Dvaput kliknite na **Politike podataka** i desno-kliknite na **SalestoRemote** i izaberite **Svojstva**.
8. Na stranici Općenito, obrišite **Upotreba Diffie-Hellman savršene tajnovitosti prosljeđivanja**.
9. Izaberite **ESP prijedlog**, kliknite **Uređivanje**.
10. Na stranici Prijedlog politike podataka, promijenite opcije kako slijedi:
    - **Način sažimanja:** Prijenos
    - **Istek ključa:** 15 minuta
    - **Ističe na granici veličine:** 100000
11. Na granici Pretvaranje, kliknite **Dodavanje**.
12. Na stranici Dodavanje pretvorbe politike podataka, izaberite sljedeće opcije:
    - **Protokol:** Sažimanje sigurnosnog korisnog sadržaja (ESP)
    - **Algoritam provjere autentičnosti:** MD5
    - **Algoritam šifriranja:** DES-CBC
13. Dvaput kliknite **OK**.

Aktiviranje pravila filtera

Čarobnjak automatski kreira paketna pravila koja ova veza zahtijeva za ispravan rad. Međutim, morate ih aktivirati na oba sistema prije nego pokrenete vezu virtualne privatne mreže (VPN).

Da aktivirate pravila filtera na Sistemu A, slijedite ove korake:

Važno: IP adrese korištene u ovom scenariju su samo u svrhu primjera. One ne odražavaju shemu IP adresiranja i ne bi se trebale koristiti ni u jednoj stvarnoj konfiguraciji. Kod dovršavanja ovih zadataka trebate koristiti vlastite IP adrese.

1. Iz System i Navigator, proširite ***Sistem A*** → **Mreža** → **IP politike**.
2. Desno-kliknite **Paketna pravila** i izaberite **Aktiviranje pravila**.
3. Na stranici Aktiviranje paketnih pravila izaberite **aktiviranje samo VPN generiranih pravila** i izaberite **ETHLINE** kao sučelje na kojem želite aktivirati ova pravila filtera. Kliknite **OK**.

Prije nego udaljeni korisnici mogu konfigurirati svoje Windows XP radne stanice, administrator im daje sljedeće informacije da mogu postaviti svoju stranu veze. Svakom od vaših udaljenih korisnika dajte sljedeće informacije:

- Naziv preddijeljenog ključa: mycokey
- IP adresu Sistema A: 192.168.1.2 (2001:DB8::2 u IPv6)
- Korisničko ime i lozinku za vezu

Bilješka: Ovo je kreirano kada je administrator dodao korisničko ime i lozinke validacijskoj listi za vrijeme konfiguracije Layer Two Tunneling Protocol (L2TP) profila završnog dijela programa.

Konfiguriranje VPN-a na Windows XP klijentu

Koristite ovaj postupak da konfigurirate VPN na Windows XP klijentu.

Udaljeni korisnici na MyCo, Inc trebaju postaviti svoj udaljeni Windows XP klijent dovršenjem sljedećih koraka:

1. U Windows XP **Start** izborniku proširite **All Programs** → **Accessories** → **Communications** → **New Connection Wizard**.
2. Na stranici dobrodošlice pročitajte informacije pregleda. Kliknite **Sljedeće**.
3. Na stranici Tipa povezivanja mreže izaberite **Spoji na mrežu na mom radnom mjestu**. Kliknite **Sljedeće**.
4. Na stranici povezivanja mreže izaberite **povezivanje Virtualne privatne mreže**. Kliknite **Sljedeće**.
5. Na stranici Naziv povezivanja, unesite Povezivanje na ogranak ureda u polju **Naziv poduzeća**. Kliknite **Sljedeće**.
6. Na stranici Javne mreže, izaberite **Nemojte birati početno povezivanje**. Kliknite **Sljedeće**.
7. Na stranici Izbora VPN poslužitelja, unesite 192.168.1.2 (2001:DB8::2 u IPv6) u polje **Host ime ili IP adresa**. Kliknite **Sljedeće**.
8. Na stranici Dostupnost veze, izaberite **Samo moja upotreba**. Kliknite **Sljedeće**.
9. Na stranici Sažetak, kliknite **Dodajte prečicu do ove veze na moj desktop**. Kliknite **Završetak**.
10. Kliknite ikonu **Spoji vezu na MyCo** koja je kreirana na vašem desktopu.
11. Na stranici Spajanje veze na MyCo, unesite korisničko ime i lozinku koje ste dobili od administratora.
12. Izaberite **Spremi ovo korisničko ime i lozinku za sljedeće korisnike** i **Samo ja**. Kliknite **Svojstva**.
13. Na stranici **Sigurnost**, osigurajte da je osigurano sljedeće **Sigurnosne opcije**:
    - **Tipično**
    - **Potrebna sigurnosna lozinka**
    - **Potrebno šifriranje podataka**

    Kliknite **IPSec postavke**.
14. Na stranici IPSec postavki izaberite **Koristite preddijeljeni ključ za provjeru autentičnosti** i unesite mycokey u polje **Preddijeljeni ključ**. Kliknite **OK**.
15. Na stranici Umrežavanje, izaberite **L2TP IPSec VPN** kao **VPN tip**. Kliknite **OK**.
16. Prijavite se s korisničkim imenom i lozinkom i kliknite na **Povezivanje**.

Da bi pokrenuli povezivanje virtualne privatne mreže (VPN) na strani klijenta, kliknite ikonu koja se pojavljuje na vašem desktopu nakon dovršenja čarobnjaka povezivanja.

Testiranje VPN veze između krajnjih točaka

Nakon završetka konfiguriranja veze između Sistema A i udaljenih korisnika i uspješno pokrenute veze, trebali bi testirati povezanost da osigurate da udaljeni hostovi mogu komunicirati jedan s drugim.

Da testirate povezanost, slijedite ove korake:

1. Iz System i Navigator, proširite ***Sistem A*** → **Mreža**.
2. Desno kliknite **TCP/IP Konfiguracija** i izaberite **Pomoćni programi** i nakon toga izaberite **Ping**.
3. Iz kućice dijaloga **Ping sa**, unesite 10.1.1.101 (2001:DA8::1:101 u IPv6) u polje **Ping**.

   Bilješka: 10.1.1.101 predstavlja IP adresu dinamički dodijeljenu (udaljenom klijentu prodaje) iz spremišta adresa, navedenu u Layer Two Tunneling Protocol (L2TP) profilu završnog dijela programa na Sistemu A.
4. Kliknite **Ping sada** da provjerite povezanost od Sistema A do udaljene radne stanice. Kliknite na **OK**.

Da testirate vezu s udaljenog klijenta, udaljeni zaposlenik dovršava ove korake na radnoj stanici koja izvodi Windowse:

1. Iz prompta za naredbe, unosi ping 10.1.1.2 (ping 2001:DA8::2 u IPv6). To je IP adresa jedne od radnih stanica u mreži korporativnog ureda.
2. Ponovite ove korake da testirate povezanost iz korporativnog ureda do ureda podružnice.

Scenarij: Upotreba prijevoda mrežne adrese za VPN

U ovom scenariju, poduzeće želi razmijeniti osjetljive podatke s jednim od poslovnih partnera koristeći VPN. Da bi se zaštitila privatnost mrežne strukture poduzeća, vaše poduzeće će također koristiti VPN NAT za skrivanje IP adresa sistema koje koristi za host aplikacija i na kojem poslovni partner ima pristup.

Situacija

Pretpostavite da ste administrator mreže za malo proizvodno poduzeće u Minneapolisu. Jedan od vaših poslovnih partnera, dostavljača dijelova u Chicagu, želi započeti nešto više od posla s vašim poduzećem preko Interneta. Od kritične je važnosti da vaše poduzeće ima određene dijelove i količinu točno u trenutku kada ih treba, tako da dobavljač treba biti svjestan stanja u inventaru vašeg poduzeća i rasporeda proizvodnje. Trenutno ovakvom interakcijom rukujete ručno, ali smatrate ju vremenski dugotrajnom, skupom, čak povremeno i netočnom, stoga ste i više nego voljni istražiti i druge opcije.

S obzirom na povjerljivost i vremenski osjetljivu prirodu informacija koje razmjenjujete, odlučili ste kreirati VPN između mreža vašeg dobavljača i vašeg poduzeća. Da bi se zaštitila privatnost mrežne strukture poduzeća, odlučujete da trebate sakriti IP adresu sistema koji je host za aplikacije na koje poslovni partner ima pristup.

VPN-ove možete koristiti ne samo za kreiranje definicija veze VPN gatewaya u mreži vašeg poduzeća, nego i za osiguranje prevođenja adresa koje treba sakriti vaše privatne lokalne adrese. Za razliku od konvencionalnog prijevoda mrežne adrese (NAT), koji mijenja IP adrese u sigurnosnim asocijacijama (SA) koje VPN zahtijeva za funkcioniranje, VPN NAT obavlja prijevod adresa prije SA provjere valjanosti, dodjelom adrese vezi kada se veza pokrene.

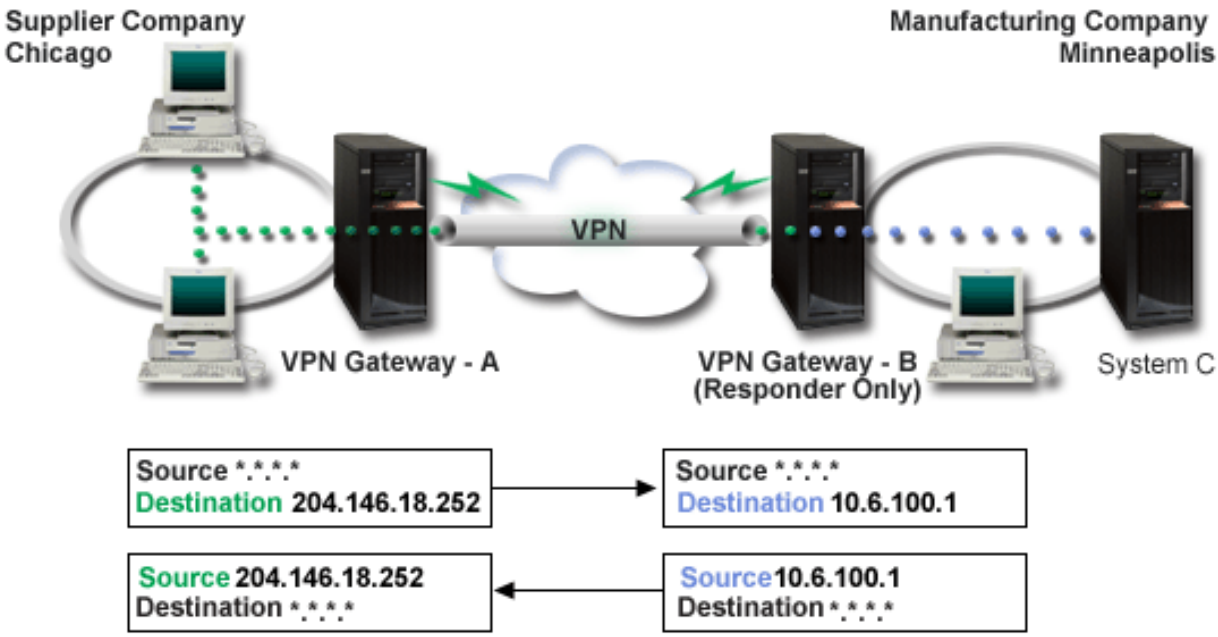
Ciljevi

Glavni ciljevi ovog scenarija su:

- omogućavanje pristupa klijentima u mreži opskrbljivača pojedinačnom host sistemu u mreži proizvođača preko gateway-to-gateway VPN veze.
- skrivanje privatnih IP adresa host sistema u mreži proizvođača, njihovim prevođenjem u javne IP adrese korištenjem prevođenja mrežne adrese za VPN (VPN NAT).

Detalji

Sljedeći dijagram pokazuje mrežne karakteristike mreže opskrbljivača i mreže proizvođača:



- VPN prilaz-A je konfiguriran da uvijek započne veze na VPN prilaz-B.
- VPN prilaz-A definira krajnju točku odredišta za vezu poput 204.146.18.252 (javna adresa dodijeljena Sistemu C).
- Sistem C ima privatnu IP adresu u mreži proizvođača 10.6.100.1.
- Javna adresa 204.146.18.252 je definirana u lokalnom spremištu usluga na VPN prilazu-B za privatnu adresu Sistema C, 10.6.100.1.
- VPN prilaz-B prevodi javnu adresu Sistema C na njegovu privatnu adresu 10.6.100.1, za ulazne datograme. VPN prilaz-B prevodi vraćajuće, odlazeće datograme s 10.6.100.1 natrag na javnu adresu Sistema C, 204.146.18.252. Onoliko koliko su klijenti u mreži dobavljača uključeni, Sistem C ima IP adresu 204.146.18.252. Oni nikad neće biti svjesni da se desio prijevod adresa.

Zadaci konfiguracije

Morate dovršiti svaki od ovih zadataka da konfigurirate vezu koja se opisuje ovim scenarijem:

1. Konfiguriranje osnovnog prilaz-prilaz VPN-a između **VPN prilaza-A** i **VPN prilaza-B**.
2. Definiranje lokalnog servisnog spremišta na **VPN prilazu-B**, za skrivanje privatne adrese **Sistema C**, iza javnog identifikatora 204.146.18.252.
3. Konfiguriranje **VPN prilaza-B** da prevede lokalne adrese koristeći adrese spremišta za lokalne usluge.

Srodni koncepti

"Prijevod mrežne adrese za VPN" na stranici 8
VPN daje načine izvođenja prevođenja mrežnih adresa, zvanih VPN NAT. VPN NAT se razlikuje od tradicionalnog NAT-a u tome što prevodi adrese prije nego primjeni IKE i IPSec protokole. Obratite se na ovo poglavlje da naučite više.

Planiranje za VPN

Prvi korak uspješnog korištenja VPN-a je planiranje. Ovo poglavlje sadrži informacije o migraciji iz prijašnjih izdanja, potrebama postava i vezama na savjetnika planiranja koji će generirati radnu tablicu planiranja koja je prilagođena vašim specifikacijama.

Planiranje je važan dio vašeg ukupnog VPN rješenja. Mnogo je kompleksnih odluka koje morate donijeti da osigurate da vaša veza radi ispravno. Koristite ove resurse za skupljanje svih informacija koje trebate da osigurate da je vaš VPN uspješan:

- Zahtjevi za VPN postav
- Određivanje tipa VPN-a za kreiranje
- Korištenje VPN savjetnika planiranja

  Savjetnik za planiranje vas ispituje o vašoj mreži i na osnovu vaših odgovora daje vam prijedloge za kreiranje vašeg VPN-a.

  Bilješka: Koristite ovaj savjetnik samo za veze koje podržavaju protokol Internet Key Exchange (IKE). Koristite radnu tablicu za planiranje ručnih veza za vaše tipove ručnih veza.
- Popunjavanje radnih tablica za planiranje VPN-a

Nakon što ste prikazali plan za VPN, počnite s konfiguracijom.

Srodni zadaci

Upotreba savjetnika za VPN planiranje

“Konfiguriranje VPN-a” na stranici 44
VPN sučelje vam omogućava nekoliko različitih načina za konfiguriranje vaših VPN veza. Možete konfigurirati ručnu ili dinamičku vezu.

Zahtjevi za VPN postav

Da bi VPN veza ispravno funkcionirala na vašim sistemima i s mrežnim klijentima, morate zadovoljiti minimum zahtjeva

Sljedeće ispisuje minimum zahtjeva za postavljanje VPN veze:

Sistemski zahtjevi

- i5/OS verzija 5 izdanje 3 ili kasnije
- Upravitelj digitalnih certifikata
- System i Access za Windows
- System i Navigator
  - Mrežna komponenta System i Navigator
- Postavite sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1
- TCP/IP mora biti konfiguriran, uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene

Zahtjevi klijenta

- Radna stanica s Windows 32-bit operativnim sistemom ispravno povezana na vaš sistem i konfigurirana za TCP/IP
- A 233 MHz jedinica za obradu
- 32 MB RAM za Windows 95 klijente
- 64 MB RAM za Windows NT 4.0 i Windows 2000 klijente
- System i Access za Windows i System i Navigator instaliran na PC klijentu
- Softver koji podržava protokol IP sigurnosti (IPSec)
- Softver koji podržava L2TP, ako udaljeni korisnici koriste L2TP za uspostavljanje veze s vašim sistemom

Srodni zadaci

“Kako započeti s VPN rješavanjem problema” na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Određivanje koji tip VPN-a kreirati

Određivanje kako ćete koristiti vaš VPN jedan je od prvih koraka u uspješnom planiranju. Da to napravite, trebate razumjeti ulogu koju u vezi igraju oboje, lokalni poslužitelj ključa i udaljeni poslužitelj ključa.

Na primjer, da li se krajnje točke *veze* razlikuju od krajnjih točaka *podataka*? Da li su iste ili neka kombinacija od oboje? Krajnje točke veze provjeravaju autentičnost i šifriraju (ili dešifriraju) promet podataka za vezu i opcijski omogućuju upravljanje ključem pomoću protokola Internet razmjene ključa (IKE). Krajnje točke podataka, međutim, definiraju vezu između dva sistema za IP promet koji teče preko VPN-a; na primjer sav TCP/IP promet između 123.4.5.6 i 123.7.8.9. Obično, kada su krajnje točke veze i podataka različite, VPN poslužitelj je prilaz. Kada su one iste, VPN poslužitelj je host.

Slijede različiti tipovi VPN primjena koje su dobro prilagođene većini poslovnih potreba:

Prilaz-prilaz
: Krajnje točke veze za oba sistema su različite od krajnjih točaka podataka. Protokol IP sigurnosti (IPSec) štiti promet dok putuje između dva prilaza. Međutim, IPSec ne štiti promet podataka niti na jednoj strani dva prilaza unutar internih mreža. Ovo je uobičajeni postav za veze između područnih ureda, jer promet koji je usmjeren dalje od prilaza područnih ureda, unutar interne mreže, je najčešće smatran pouzdanim.

Prilaz-host
: IPSec štiti promet podataka dok putuje između prilaza i hosta na udaljenoj mreži. VPN ne štiti promet podataka unutar lokalne mreže, zato jer ju smatrate pouzdanom.

Host-prilaz
: VPN štiti promet podataka dok putuje između hosta na lokalnoj mreži i udaljenog prilaza. VPN ne štiti promet podataka na udaljenoj mreži.

Host-host
: Krajnje točke veze iste su kao i krajnje točke podataka na oba sistema, lokalnom i udaljenom. VPN štiti promet podataka dok putuje između hosta na lokalnoj mreži i hosta na udaljenoj mreži. Ovaj tip VPN-a daje IPSec zaštitu od jednog do drugog kraja.

Dovršenje radnih tablica VPN planiranja

Koristite radije radne tablice VPN planiranja za dohvaćanje detaljnih informacija o vašim planovima VPN upotrebe. Morate dovršiti ove radne tablice za prikladan plan vaše VPN strategije. Ove informacije možete također koristiti da konfigurirate vaš VPN.

Ako preferirate, možete ispisati i dovršiti radne tablice planiranja za dohvaćanje detaljnih informacija o vašim VPN planovima upotrebe.

Izaberite radnu tablicu za tip veze koju želite kreirati.

- Planiranje radne tablice za dinamičke veze
- Planiranje radne tablice za ručna povezivanja
- Savjetnik za planiranje VPN-a

  Ili, ako želite, koristite savjetnika za interaktivno planiranje i vođenje kroz konfiguraciju. Savjetnik za planiranje vas ispituje o vašoj mreži i na osnovu vaših odgovora daje vam prijedloge za kreiranje vašeg VPN-a.

  Bilješka: VPN savjetnik planiranja koristite samo da dinamičke veze. Koristite radnu tablicu planiranja za ručne veze, za tipove ručnog povezivanja.

Ako ćete kreirati više veza sa sličnim svojstvima, možda ćete željeti postaviti VPN defaulte. Default vrijednosti koje konfigurirate ispunjavaju listove za VPN svojstva. Ovo znači da ne trebate konfigurirati ista svojstva više puta. Da postavite VPN default vrijednosti, izaberite **Uredi** iz glavnog izbornika VPN-a, a zatim izaberite **Default vrijednosti**.

Srodne informacije

Savjetnik za planiranje VPN-a

Planiranje radne tablice za dinamičke veze

Dovršite ovu radnu tablicu prije konfiguriranja dinamičke veze.

Prije kreiranja vaših dinamičkih VPN veza, dovršite ovu radnu tablicu. Radna tablica pretpostavlja da ćete koristiti Čarobnjaka nove veze. Čarobnjak vam dozvoljava da postavite VPN na osnovu vaših osnovnih zahtjeva sigurnosti. U nekim slučajevima ćete možda trebati preraditi svojstva koja čarobnjak konfigurira za vezu. Na primjer, možda ćete odlučiti da trebate vođenje dnevnika ili da želite da se VPN poslužitelj pokrene svaki put kada se TCP/IP pokrene. Ako je to slučaj, desno kliknite na grupu dinamičkog ključa ili vezu koju je čarobnjak izabrao i izaberite **Svojstva**.

Odgovorite na svako pitanje prije nego nastavite s postavljanjem VPN-a.

Tablica 9. Sistemski zahtjevi

Kontrolna lista preduvjeta	**Odgovori**
Je li vaš operativni sistem i5/OS V5R3 ili kasniji?	Da
Je li Upravitelj digitalnih certifikata opcija instalirana?	Da
Da li je instaliran System i Access za Windows?	Da
Da li je instaliran System i Navigator?	Da
Da li je instalirana mrežna pomoćna komponenta System i Navigator ?	Da
Da li je instaliran IBM TCP/IP pomoćni programi povezanosti za i5/OS?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na sistemu (uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene)?	Da
Da li je uspostavljena normalna TCP/IP komunikacija između zahtijevanih krajnjih točaka?	Da
Jeste li primijenili privremene popravke za posljednji program (PTF-ove)?	Da
Ako VPN tunel prolazi kroz vatrozid ili usmjerivače koji koriste IP filtriranje, da li pravila filtriranja vatrozida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatrozidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	Da
Da li su vatrozidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Tablica 10. VPN konfiguracija

Ove informacije trebate za konfiguraciju VPN veze	**Odgovori**
Koji tip veze kreirate? • Prilaz-prilaz • Host-prilaz • Prilaz-host • Host-host	
Kako ćete nazvati grupu dinamičkog ključa?	
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših ključeva? • Najviša sigurnost, najniža izvedba • Balance sigurnost i izvedba • Najniža sigurnost i najviša izvedba	
Da li koristite certifikate za provjeru autentičnosti veze? Ako ne, koji je unaprijed podijeljeni ključ?	
Koji je identifikator za lokalnog poslužitelja ključa?	
Koji je identifikator za lokalnog poslužitelja ključa?	
Koji je identifikator udaljenog poslužitelja ključa?	
Koji je identifikator za udaljenu krajnju točku podataka?	

Tablica 10. VPN konfiguracija (nastavak)

Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka? • Najviša sigurnost, najniža izvedba • Balance sigurnost i izvedba • Najniža sigurnost i najviša izvedba	

Planiranje radne tablice za ručna povezivanja

Dovršite ovu radnu tablicu prije konfiguriranja ručnog povezivanja.

Dovršite ovu radnu tablicu da vam pomogne u kreiranju vaših veza virtualne privatne mreže (VPN), koje ne koriste IKE za upravljanje ključeva. Odgovorite na svako pitanje prije nego nastavite s postavljanjem VPN-a:

Tablica 11. Sistemski zahtjevi

Kontrolna lista preduvjeta	**Odgovori**
Izvodi li sistem i5/OS V5R3, ili kasniju?	
Je li Upravitelj digitalnih certifikata instaliran?	
Da li je instaliran System i Access za Windows?	
Da li je instaliran System i Navigator?	
Da li je instalirana mrežna pomoćna komponenta System i Navigator ?	
Da li je instaliran IBM TCP/IP pomoćni programi povezanosti za i5/OS?	
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	
Da li je TCP/IP konfiguriran na sistemu (uključujući IP sučelja, smjerove, ime lokalnog hosta i ime lokalne domene)?	
Da li je uspostavljena normalna TCP/IP komunikacija između zahtijevanih krajnjih točaka?	
Jeste li primijenili privremene popravke za posljednji program (PTF-ove)?	
Ako VPN tunel prolazi kroz vatrozid ili usmjerivače koji koriste IP filtriranje, da li pravila filtriranja vatrozida ili usmjerivača podržavaju AH i ESP protokole?	
Da li su vatrozidovi ili usmjerivači konfigurirani da dozvole AH i ESP protokole?	
Da li su vatrozidovi konfigurirani da omoguće IP prosljeđivanje?	

Tablica 12. VPN konfiguracija

Ove informacije trebate za konfiguraciju ručne VPN veze	**Odgovori**
Koji tip veze kreirate? • Host-host • Host-prilaz • Prilaz-host • Prilaz-prilaz	
Kako ćete nazvati vezu?	
Koji je identifikator za lokalnu krajnju točku veze?	
Koji je identifikator za udaljenu krajnju točku veze?	
Koji je identifikator za lokalnu krajnju točku podataka?	
Koji je identifikator za udaljenu krajnju točku podataka?	
Koji ćete tip prometa dozvoliti za ovu vezu (lokalni port, udaljeni port i protokol)?	
Da li zahtijevate prijevod adrese za ovu vezu? Pogledajte prijevod mrežne adrese VPN-a za više informacije.	

Tablica 12. VPN konfiguracija (nastavak)

Da li ćete koristiti tunelski ili transportni način?	
Koji će IPSec protokol veza koristiti (AH, ESP ili AH s ESP)? Pogledajte IP sigurnost (IPSec) za više informacija.	
Koji algoritam za provjeru autentičnosti će veza koristiti (HMAC-MD5 ili HMAC-SHA)?	
Koji algoritam za šifriranje će veza koristiti (DES-CBC ili 3DES-CBC)? **Bilješka:** Navedite algoritam šifriranja samo ako ste izabrali ISP kao IPSec protokol.	
Što je AH ulazni ključ? Ako koristite MD5, ključ je 16-bajtni heksadecimalni niz. Ako koristite SHA, ključ je 20-bajtni heksadecimalni niz. Vaš ulazni ključ mora se točno podudarati s izlaznim ključem udaljenog poslužitelja.	
Što je AH izlazni ključ? Ako ćete koristiti MD5, ključ je 16-bajtni heksadecimalni niz. Ako ćete koristiti SHA, ključ je 20-bajtni heksadecimalni niz. Vaš izlazni ključ mora se točno podudarati s ulaznim ključem udaljenog poslužitelja.	
Što je ESP ulazni ključ? Ako koristite DES, ključ je 8-bajtni heksadecimalni string. Ako ćete koristiti 3DES, ključ je 24-bajtni heksadecimalni niz. Vaš ulazni ključ mora se točno podudarati s izlaznim ključem udaljenog poslužitelja.	
Što je ESP izlazni ključ? Ako koristite DES, ključ je 8-bajtni heksadecimalni string. Ako ćete koristiti 3DES, ključ je 24-bajtni heksadecimalni niz. Vaš izlazni ključ mora se točno podudarati s ulaznim ključem udaljenog poslužitelja.	
Što je ulazni Indeks politike sigurnosti (SPI)? Ulazni SPI je 4-bajtni heksadecimalni niz, gdje je prvi bajt postavljen na 00. Vaš ulazni SPI mora se točno podudarati s izlaznim SPI-jem udaljenog poslužitelja.	
Što je izlazni SPI? Izlazni SPI je 4-bajtni heksadecimalni niz. Vaš izlazni SPI mora se točno podudarati s ulaznim SPI-jem udaljenog poslužitelja.	

Srodni koncepti

“Prijevod mrežne adrese za VPN” na stranici 8
VPN daje načine izvođenja prevođenja mrežnih adresa, zvanih VPN NAT. VPN NAT se razlikuje od tradicionalnog NAT-a u tome što prevodi adrese prije nego primjeni IKE i IPSec protokole. Obratite se na ovo poglavlje da naučite više.

Konfiguriranje VPN-a

VPN sučelje vam omogućava nekoliko različitih načina za konfiguriranje vaših VPN veza. Možete konfigurirati ručnu ili dinamičku vezu.

Dinamička veza je ona koja dinamički generira i dogovara ključeve koji osiguravaju vašu vezu, dok je ona aktivna, korištenjem Internet Key Exchange (IKE) protokola. Dinamičke veze dobavljaju posebnu razinu sigurnosti za podatke koji njom protječu jer se ključevi automatski razmjenjuju, u pravilnim intervalima. Kao posljedica, manje je vjerojatno da bi mogući napadač mogao uhvatiti ključ, imati vremena razbiti ga i koristiti ga za skretanje ili hvatanje prometa koji ključ štiti.

Ručno povezivanje, međutim, ne osigurava podršku za IKE dogovore i prema tome ni za automatsko upravljanje ključeva. Nadalje, oba kraja veze zahtijevaju od vas da konfigurirate nekoliko atributa koji se točno moraju podudarati. Ručne veze koriste statičke ključeve koji se ne osvježavaju ili mijenjaju za vrijeme dok je veza aktivna. Ručnu vezu morate zaustaviti da promijenite njoj pridruženi ključ. Ako razmotrite ovaj sigurnosni rizik, možda ćete umjesto toga htjeti kreirati dinamičku vezu.

Srodni koncepti

"Planiranje za VPN" na stranici 39
Prvi korak uspješnog korištenja VPN-a je planiranje. Ovo poglavlje sadrži informacije o migraciji iz prijašnjih izdanja, potrebama postava i vezama na savjetnika planiranja koji će generirati radnu tablicu planiranja koja je prilagođena vašim specifikacijama.

Konfiguriranje VPN veza s Čarobnjakom nove veze

Čarobnjak za nove veze vam dozvoljava da kreirate virtualnu privatnu mrežu (VPN) između bilo koje od kombinacija hosta i prilaza.

Na primjer, host-host, prilaz-host, host-prilaz ili prilaz-prilaz.

Čarobnjak automatski kreira svaki od konfiguracijskih objekata koje VPN zahtijeva za ispravan rad, uključujući i paketna pravila. Međutim, ako trebate dodati funkciju na vaš VPN; na primjer, vođenje dnevnika ili prijevod mrežne adrese za VPN (VPN NAT), možda ćete dalje htjeti preraditi vaš VPN preko listova papira svojstva odgovarajuće grupe dinamičkog ključa ili veze. Da ovo napravite, najprije morate zaustaviti vezu ako je aktivna. Zatim, desno kliknite grupu dinamičkog ključa ili veze i izaberite **Svojstva**.

Dovršite savjetnik VPN planiranja prije nego počnete. Savjetnik vam daje sredstva za skupljanje važnih informacija koje ćete trebati za kreiranje vašeg VPN-a.

Da kreirate VPN pomoću Čarobnjaka veze, slijedite ove korake:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Nova veza** da pokrenete Čarobnjaka.
3. Dovršite čarobnjaka da kreirate osnovnu VPN vezu. Kliknite **Pomoć** ako zatrebate pomoć.

Srodni zadaci

Savjetnik za planiranje VPN-a

Konfiguriranje VPN sigurnosnih politika

Nakon što odredite kako ćete koristiti vaš VPN, morate definirati vaše politike VPN sigurnosti.

Bilješka: Nakon konfiguriranja VPN sigurnosnih politika, morate konfigurirati sigurne veze.

Srodni zadaci

"Konfiguriranje sigurne VPN veze" na stranici 47
Nakon što ste konfigurirali politike sigurnosti za vašu vezu morate konfigurirati sigurnu vezu.

Konfiguriranje politike Internet razmjene ključa

Politika Internet razmjene ključa (IKE) definira koju razinu provjere autentičnosti i zaštite šifriranja IKE koristi za vrijeme faze 1 dogovora.

IKE faza 1 uspostavlja ključeve koji štite poruke koje protječu u pregovore sljedeće faze 2. Ne trebate definirati IKE politiku kada kreirate ručnu vezu. Dodatno, ako kreirate vaš VPN pomoću Čarobnjaka za nove veze, čarobnjak može kreirati vašu IKE politiku za vas.

VPN koristi ili RSA način potpisa ili unaprijed podijeljeni ključ za provjeru autentičnosti pregovora faze 1. Ako planirate koristiti digitalne certifikate za provjeru autentičnosti ključnih poslužitelja, morate ih prvo konfigurirati upotrebom Upravitelj digitalnih certifikata. IKE politika također identificira koji će udaljeni poslužitelj ključa koristiti ovu politiku.

Da definirate IKE politiku ili napravite promjene na postojećoj, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → IP politike sigurnosti**.

2. Da kreirate novu politiku, desno kliknite **Politike Internet razmjene ključeva** i izaberite **Nova politika Internet razmjene ključa**. Da napravite promjene na postojećoj politici, kliknite **Politika Internet razmjene ključeva** u lijevom oknu, zatim desno kliknite politiku koju želite promijeniti u desnom oknu i izaberite **Svojstva**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Preporučljivo je da koristite glavni način pregovaranja kad god se dijeljeni ključ koristi za provjeru autentičnosti. On daje najsigurniju razmjenu. Ako morate koristiti dijeljene ključeve i agresivniji način pregovaranja, izaberite takve lozinke koje će se teško otkriti pri napadima koji koriste rječnik za otkrivanje lozinki. Također se preporučuje da periodički mijenjate vaše lozinke. Za prisilu korištenja glavnog načina pregovora pri razmjeni ključeva obavite sljedeće zadatke:

1. U System i Navigator, proširite **sistem → Mreža → IP politike.**
2. Izaberite **Virtualno privatno umrežavanje → IP politike sigurnosti → Politike razmjene Internet ključeva** za pregled trenutno definiranih politika razmjene ključeva u desnom prozoru.
3. Desno kliknite na pojedinačnu politiku razmjene ključa i izaberite **Svojstva**.
4. Na stranici Pretvorba, kliknite na **Odgovarajuća politika**. Pojavit će se dijalog Politika odgovarajuće razmjene Internet ključeva.
5. U polju Zaštita identiteta, odznačite **IKE agresivni način pregovaranja (bez zaštite identiteta)**.
6. Kliknite **OK** za povratak na dijalog Svojstva.
7. Kliknite **OK** ponovno za spremanje promjena.

Bilješka: Kada postavite polje zaštita identiteta, promjena je važeća za sve razmjene s poslužiteljima udaljenih ključeva, jer postoji samo jedna odgovarajuća IKE politika za cijeli sistem. Glavni način pregovaranja osigurava da početni sistem može zatražiti samo politiku glavnog načina razmjene ključa.

Srodni koncepti

“Upravljanje ključevima” na stranici 6
Dinamički VPN daje dodatnu sigurnost za vaše komunikacije korištenjem protokola Internet razmjena ključa (IKE) za upravljanje ključem. IKE dozvoljava VPN poslužiteljima na svakom kraju veze da pregovaraju nove ključeve u određenim intervalima.

Srodni zadaci

Upravitelj digitalnih certifikata

Konfiguriranje politike podataka

Politika podataka definira koja razina provjere autentičnosti ili šifriranja štiti podatke dok protječu kroz VPN.

Komunikacijski sistemi se slažu oko ovih atributa za vrijeme protokola Internet razmjene ključeva (IKE) pregovora faze 2. Ne trebate definirati politiku podataka kada kreirate ručnu vezu. Dodatno, ako kreirate vaš VPN pomoću Čarobnjaka za nove veze, čarobnjak može za vas kreirati vašu politiku podataka.

Da definirate politiku podataka ili napravite promjene na postojećoj, slijedite korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → IP politike sigurnosti**.
2. Da kreirate novu politiku podataka, desno kliknite **Politika podataka** i izaberite **Nova politika podataka**. Da napravite promjene na postojećoj politici podataka, kliknite **Politike podataka** (u lijevom oknu), zatim desno kliknite na politike podataka koje želite promijeniti (u desnom oknu) i izaberite **Svojstva**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Srodni koncepti

"Upravljanje ključevima" na stranici 6
Dinamički VPN daje dodatnu sigurnost za vaše komunikacije korištenjem protokola Internet razmjena ključa (IKE) za upravljanje ključem. IKE dozvoljava VPN poslužiteljima na svakom kraju veze da pregovaraju nove ključeve u određenim intervalima.

Konfiguriranje sigurne VPN veze

Nakon što ste konfigurirali politike sigurnosti za vašu vezu morate konfigurirati sigurnu vezu.

Za dinamičke veze, objekt sigurne veze uključuje grupu dinamičkog ključa i vezu dinamičkog ključa.

Grupa dinamičkog ključa definira zajedničke karakteristike jedne ili više VPN veza. Konfiguriranje grupe dinamičkog ključa vam dozvoljava korištenje iste politike, ali različitih krajnjih točki podataka za svaku vezu unutar grupe. Grupa dinamičkog ključa vam također dozvoljava da uspješno pregovarate s udaljenim inicijatorima kada krajnje točke podataka predložene od udaljenog sistema nisu unaprijed određeno poznate. Ona to čini pridruživanjem informacija politike u grupi dinamičkog ključa s pravilom filtriranja politike s tipom akcije IPSEC. Ako određene krajnje točke podataka ponuđene od udaljenog inicijatora padnu unutar raspona navedenog u IPSEC pravilu filtriranja, one mogu biti podložne politici definiranoj u grupi dinamičkog ključa.

Veza dinamičkog ključa definira karakteristike pojedinačnih veza podataka između parova krajnjih točaka. Veza dinamičkog ključa postoji unutar grupe dinamičkog ključa. Nakon što ste konfigurirali grupu dinamičkog ključa za opis politika koje koriste veze u grupi, morate kreirati individualne veze dinamičkog ključa za veze koje započinjete lokalno.

Za konfiguriranje objekt sigurnosne veze, dovršite zadatke dijela 1 i 2:

Srodni koncepti

"Konfiguriranje VPN sigurnosnih politika" na stranici 45
Nakon što odredite kako ćete koristiti vaš VPN, morate definirati vaše politike VPN sigurnosti.

"Konfiguriranje VPN paketnih pravila" na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Srodni zadaci

"Aktiviranje VPN paketnih pravila" na stranici 52
Morate aktivirati VPN paketna pravila prije nego možete pokrenuti vaše VPN veze.

Dio 1: Konfiguriranje grupe dinamičkog ključa

1. U System i Navigator, proširite **sistem → Mrežu → IP politike → Virtualno privatno umrežavanje → Sigurne veze**.
2. Desno kliknite **Po grupi** i izaberite **Nova grupa dinamičkog ključa**.
3. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Dio 2: Konfiguriranje veze dinamičkog ključa

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze → Po grupi**.
2. U lijevom dijelu System i Navigator prozora, desno kliknite na grupu dinamičkog ključa koju ste kreirali u prvom dijelu i izaberite **Nova veza dinamičkog ključa**.
3. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Nakon što ste dovršili ove korake, trebate aktivirati pravila paketa kako bi se omogućilo da veza radi pravilno.

Bilješka: U većini slučajeva, dozvolite VPN sučelju da automatski generira VPN pravila paketa, izborom opcije **Generiraj sljedeći filter politike za ovu grupu** na stranici **Grupa dinamičkog ključa - Veze**. Međutim,

ako izaberete opciju **Pravilo filtera politike će biti definirano u Pravilima paketa**, morate konfigurirati VPN pravila paketa korištenjem editora Pravila paketa i potom ih aktivirati.

Konfiguriranje ručne veze

Ručna veza je ona gdje morate konfigurirati sva vaša VPN svojstva bez upotrebe čarobnjaka.

Nadalje, oba kraja veze zahtijevaju od vas da konfigurirate nekoliko elemenata koji se moraju *točno* podudarati. Na primjer, vaši ulazni ključevi moraju se podudarati s ulaznim ključevima udaljenog sistema ili veza neće uspjeti.

Ručne veze koriste statičke ključeve koji se ne osvježavaju ili mijenjaju za vrijeme dok je veza aktivna. Ručnu vezu morate zaustaviti da bi promijenili njoj pridruženi ključ. Ako uzmete u obzir ovaj sigurnosni rizik i oba kraja veze podržavaju protokol Internet razmjene ključa (IKE), možda ćete htjeti razmotriti postavljanje dinamičke veze umjesto toga.

Da definirate svojstva za vašu ručnu vezu, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mrežu → IP politike → Virtualno privatno umrežavanje → → Sigurne veze**.
2. Desno kliknite na **Sve veze** i izaberite **Nova ručna veza**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Bilješka: U većini slučajeva, dozvolite VPN sučelju da automatski generira VPN pravila paketa izborom opcije **Generiraj filter politike koji odgovara krajnjim točkama podataka** na stranici **Ručna veza - Veza**. Međutim, ako izaberete opciju **Pravilo filtera politike će biti definirano u Pravilima paketa**, morate ručno konfigurirati pravila paketa politike i potom ih aktivirati.

Srodni zadaci

“Konfiguriranje pravila filtera politike” na stranici 50
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

Konfiguriranje dinamičke veze

Dinamička veza dinamički generira i dogovara ključeve koji osiguravaju vašu vezu dok je ona aktivna, upotrebom protokola Internet razmjene ključa (IKE).

Dovršite Čarobnjaka veze novog dinamičkog ključa za konfiguriranje dinamičke veze, slijedeći ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze → Po grupi**.
2. Desno-kliknite na određenu grupu dinamičkog ključa i izaberite **Veza novog dinamičkog ključa**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** za spremanje promjena.

Konfiguriranje VPN paketnih pravila

Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Ako odlučite kreirati VPN pravila paketa korištenjem editora Pravila paketa u System i Navigator, kreirajte također bilo koja dodatna pravila na ovaj način. Odnosno, ako ste pustili VPN da kreira vaša pravila filtera politika, kreirajte sva dodatna pravila filtera politika na isti način.

Općenito, VPN zahtijeva dva tipa pravila filtriranja: Pred-IPSec pravila filtriranja i pravila filtriranja politike. Pregledajte donja poglavlja da naučite konfigurirati ta pravila korištenjem editora Pravila paketa u System i Navigator. Ako želite čitati o ostalim VPN i opcijama filtriranja, pogledajte odjeljak VPN i IP filtriranje u poglavlju VPN koncepti.

- Konfiguriranje pred-IPSec pravila filtriranja

  Pred-IPSec pravila su bilo koja pravila na vašem sistemu koja dolaze prije pravila s tipom akcije IPSEC. Ovo poglavlje raspravlja samo o pred-IPSec pravilima koja VPN zahtijeva za ispravan rad. U ovom slučaju, pred-IPSec pravila su par pravila koja dozvoljavaju da IKE radi obradu preko veze. IKE dozvoljava pojavu generacije dinamičkog ključa i pregovora za vašu vezu. Možda ćete trebati dodati druga pred-IPSec pravila ovisno o vašoj određenoj mrežnoj okolini i sigurnosnoj politici.

  Bilješka: Trebate konfigurirati ovaj tip pred-IPSec pravila ako već imate ostala pravila koja dozvoljavaju IKE za navedene sisteme. Ako nema pravila filtriranja na sistemu napisanih sa svrhom dozvole IKE prometa, tada je IKE promet uključeno dozvoljen.
- Konfiguriranje pravila filtriranja politike

  Pravilo filtriranja politike definira promet koji može koristiti VPN i koju politiku za zaštitu podataka treba primijeniti na taj promet.

Stvari koje morate uzeti u obzir prije početka

Kada dodate pravila filtriranja na sučelje, sistem automatski dodaje default DENY pravilo za to sučelje. To znači da je zabranjen bilo kakav promet koji izričito nije dozvoljen. Ovo pravilo ne možete vidjeti ili mijenjati. Kao rezultat ćete možda otkriti da promet koji je prethodno radio, misteriozno ne uspijeva nakon aktiviranja vaših VPN pravila filtera. Ako na sučelju želite dozvoliti promet različit od VPN-a, morate dodati izričita PERMIT pravila.

Nakon konfiguracije odgovarajućih pravila filtera, morate definirati sučelje na koje se ona primjenjuju i potom ih aktivirati.

Od velike je važnosti da ispravno konfigurirate vaša pravila filtriranja. Ako ne, pravila filtera mogu blokirati sav dolazni i odlazni IP promet na sistemu. Ovo uključuje vezu na System i Navigator, koju koristite za konfiguriranje pravila filtera.

Ako pravila filtera ne dopuštaju System i promet, System i Navigator ne može komunicirati s vašim sistemom. Ako se nađete u ovoj situaciji, morate se logirati na sistem pomoću sučelja koje ima povezanost, kao što je Operacijska konzola. Koristite naredbu RMVTCPTBL da uklonite sve filtere na ovom sistemu. Ova naredba također završava *VPN poslužitelje i zatim ih ponovno pokreće. Zatim konfigurirajte vaše filtere i reaktivirajte ih.

Srodni koncepti

“VPN i IP filtriranje” na stranici 11
IP filtriranje i VPN blisko su povezani. Zapravo, većina VPN veza zahtijeva pravila filtriranja za ispravan rad. Ovo poglavlje daje vam informacije o tome koje filtere VPN zahtijeva, kao i ostale koncepte filtriranja povezane s VPN-om.

Srodni zadaci

“Konfiguriranje sigurne VPN veze” na stranici 47
Nakon što ste konfigurirali politike sigurnosti za vašu vezu morate konfigurirati sigurnu vezu.

“Konfiguriranje pred-IPSec pravila filtriranja” na stranici 50
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

“Konfiguriranje pravila filtera politike” na stranici 50
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

“Definiranje sučelja za VPN pravila filtera” na stranici 52
Nakon što konfigurirate vaša VPN paketna pravila i bilo koja druga pravila koja trebate da omogućite vašu VPN vezu, morate definirati sučelje na koje se ta pravila primjenjuju.

“Aktiviranje VPN paketnih pravila” na stranici 52
Morate aktivirati VPN paketna pravila prije nego možete pokrenuti vaše VPN veze.

Konfiguriranje pred-IPSec pravila filtriranja

Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

Par poslužitelja Internet razmjene ključeva (IKE) dinamički pregovara i osvježava ključeve. IKE koristi dobro poznati port, 500. Da bi IKE ispravno radio, trebate dozvoliti UDP datograme preko porta 500 za ovaj IP promet. Da to napravite, kreirat ćete par pravila filtriranja; jedno za ulazni promet i jedno za vanjski promet, tako da vaša veza može dinamički pregovarati ključeve da zaštiti vezu:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Pravila paketa** i izaberite **Editor pravila**. Ovo otvara editor Pravila paketa, koji vam omogućava kreiranje ili uređivanje pravila filtera ili NAT-a na sistemu.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Pravila paketa izaberite **Umetni → Filter**.
5. Na stranici **Općenito** navedite skup imena za vaša VPN pravila filtriranja. Preporučuje se da kreirate barem tri različita skupa: jedan za vaša pre-IPSec pravila, jedan za vaša pravila filtera politike i jedan za različita pravila filtera PERMIT i DENY. Imenujte skup koji sadrži vaša pravila pre-IPSec filtera s prefiksom *preipsec*. Na primjer, preipsecfilteri.
6. U polju **Akcija** izaberite **PERMIT** iz padajuće liste.
7. U polju **Smjer** izaberite **OUTBOUND** iz padajuće liste.
8. U polju **Ime adrese izvora** izaberite **=** iz prve padajuće liste i zatim upišite IP adresu lokalnog poslužitelja ključa u drugo polje. Specificirali ste IP adresu lokalnog poslužitelja ključa u IKE politici.
9. U polju **Ime adrese odredišta** izaberite **=** iz prve padajuće liste i zatim upišite IP adresu udaljenog poslužitelja ključa u drugo polje. Također ste specificirali IP adresu udaljenog poslužitelja ključa u IKE politici.
10. Na stranici **Usluge**, izaberite **Usluga**. Ovo omogućuje polja **Protokol**, **Port izvora** i **Port odredišta**.
11. U polju **Protokol** izaberite **UDP** iz padajuće liste.
12. Za **Port izvora** izaberite **=** u prvom polju, zatim u drugom polju upišite 500.
13. Ponovite prethodni korak za **Port odredišta**.
14. Kliknite **OK**.
15. Ponovite ove korake da konfigurirate INBOUND filter. Koristite isto ime skupa i obrnite adrese kao što je potrebno.

Bilješka: Manje sigurna, ali lakša opcija za dozvolu IKE prometa preko veze, je konfiguracija samo jednog pre-IPSec filtera i korištenje vrijednosti generičkih znakova (*) u poljima **Smjer**, **Ime adrese izvora** i **Ime adrese cilja**.

Sljedeći korak je konfiguracija pravila filtera politika za definiranje IP prometa koji štiti VPN veza.

Srodni koncepti

“Konfiguriranje VPN paketnih pravila” na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Srodni zadaci

“Konfiguriranje pravila filtera politike”
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

Konfiguriranje pravila filtera politike

Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

Pravilo filtriranja politike (pravilo gdje je akcija=IPSEC) definira koje adrese, protokole i portove može koristiti VPN. Također definira politiku koja će biti primijenjena na promet u VPN vezi. Za konfiguraciju pravila filtriranja politike, slijedite ove korake:

Bilješka: Ako ste upravo konfigurirali pravilo pre-IPSec (samo za dinamičke veze), editor Pravila paketa bit će i dalje otvoren; idite na korak 4.

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Pravila paketa** i izaberite **Editor pravila**. Ovo otvara editor Pravila paketa, koji vam omogućava kreiranje ili uređivanje pravila filtera ili NAT-a na sistemu.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Pravila paketa izaberite **Umetni → Filter**.
5. Na stranici **Općenito** navedite skup imena za vaša VPN pravila filtriranja. Preporučuje se da kreirate barem tri različita skupa: jedan za vaša pre-IPSec pravila, jedan za vaša pravila filtera politike i jedan za različita pravila filtera PERMIT i DENY. Na primjer, filteripolitike
6. U polju **Akcija** izaberite **IPSEC** iz padajuće liste. Polje **Smjer** postavlja se na OUTBOUND i ne možete ga promijeniti. Iako se ovo polje postavlja na OUTBOUND, ono je zapravo dvosmjerno. OUTBOUND se prikazuje da razjasni semantiku ulaznih vrijednosti. Na primjer, vrijednosti izvora su lokalne vrijednosti, a vrijednosti odredišta su udaljene vrijednosti.
7. Za **Ime adrese izvora** izaberite **=** u prvom polju, a zatim upišite IP adresu lokalne krajnje točke podataka u drugom polju. Također možete specificirati raspon IP adresa ili IP adresu plus masku podmreže nakon što ih definirate, koristeći funkciju **Definiraj adrese**.
8. Za **Ime adrese odredišta** izaberite **=** u prvom polju, a zatim upišite IP adresu udaljene krajnje točke podataka u drugom polju. Također možete specificirati raspon IP adresa ili IP adresu plus masku podmreže nakon što ih definirate, koristeći funkciju **Definiraj adrese**.
9. U polju **Vođenje dnevnika** specificirajte koju razinu vođenja dnevnika zahtijevate.
10. U polju **Ime veze** izaberite odredište veze na koju se ova pravila filtriranja odnose.
11. (opcijski) Upišite opis.
12. Na stranici **Usluge**, izaberite **Usluga**. Ovo omogućuje polja **Protokol**, **Port izvora** i **Port odredišta**.
13. U polju **Protokol**, **Port izvora** i **Port odredišta** izaberite prikladne vrijednosti za promet. Ili, možete izabrati zvjezdicu (*) iz padajuće liste. Ovo omogućuje bilo kojem protokolu da koristi VPN, neovisno o tome koji port koristi.
14. Kliknite **OK**.

Sljedeći korak je definiranje sučelja na koja će se primijeniti pravila politike.

Bilješka: Pri dodavanju pravila filtera sučelja, sistem automatski dodaje default DENY pravilo za to sučelje. To znači da je zabranjen bilo kakav promet koji izričito nije dozvoljen. Ovo pravilo ne možete vidjeti ili mijenjati. Kao rezultat ćete možda otkriti da veze na kojima ste prethodno radili misteriozno neće uspjeti nakon aktiviranja vaših VPN paketnih pravila. Ako na sučelju želite dozvoliti promet različit od VPN-a, morate dodati izričita PERMIT pravila.

Srodni koncepti

“Konfiguriranje VPN paketnih pravila” na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Srodni zadaci

“Konfiguriranje ručne veze” na stranici 48
Ručna veza je ona gdje morate konfigurirati sva vaša VPN svojstva bez upotrebe čarobnjaka.

“Konfiguriranje pred-IPSec pravila filtriranja” na stranici 50
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

“Definiranje sučelja za VPN pravila filtera” na stranici 52
Nakon što konfigurirate vaša VPN paketna pravila i bilo koja druga pravila koja trebate da omogućite vašu VPN vezu, morate definirati sučelje na koje se ta pravila primjenjuju.

Definiranje sučelja za VPN pravila filtera

Nakon što konfigurirate vaša VPN paketna pravila i bilo koja druga pravila koja trebate da omogućite vašu VPN vezu, morate definirati sučelje na koje se ta pravila primjenjuju.

Da definirate sučelje na koje primijeniti vaša VPN pravila filtriranja, slijedite ove korake:

Bilješka: Ako ste upravo konfigurirali pravila paketa za VPN, sučelje Pravila paketa bit će i dalje otvoreno; idite na korak četiri.

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Pravila paketa** i izaberite **Editor pravila**. Ovo otvara editor Pravila paketa, koji vam omogućava kreiranje ili uređivanje pravila filtera ili NAT-a na sistemu.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Pravila paketa izaberite **Umetni → Sučelje filtera**.
5. Na stranici **Općenito** izaberite **Ime linije**, zatim iz padajuće liste izaberite opis linije na koju se vaša VPN paketna pravila primjenjuju.
6. (opcijski) Upišite opis.
7. Na stranici **Skupovi filtera** kliknite **Dodaj** da dodate svako ime skupa za filtere koje ste upravo konfigurirali.
8. Kliknite **OK**.
9. Spremite vašu datoteku s pravilima. Datoteka je spremljena u integrirani sistem datoteka na vašem sistemu s ekstenzijom .i3p.

   Bilješka: Ne spremajte datoteku u sljedeći direktorij:

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

   Ovaj direktorij je samo za sistemsku upotrebu. Ako ikad zatrebate korištenje naredbe RMVTCPTBL *ALL da deaktivirate paketna pravila, naredba će obrisati sve datoteke unutar ovog direktorija.

Nakon što definirate sučelje za vaša pravila filtera, morate ih aktivirati prije nego možete pokrenuti VPN.

Srodni koncepti

“Konfiguriranje VPN paketnih pravila” na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Srodni zadaci

“Konfiguriranje pravila filtera politike” na stranici 50
Ovaj zadatak dovršite samo ako ste naveli da ne želite da VPN automatski generira pravilo filtera politike.

“Aktiviranje VPN paketnih pravila”
Morate aktivirati VPN paketna pravila prije nego možete pokrenuti vaše VPN veze.

Aktiviranje VPN paketnih pravila

Morate aktivirati VPN paketna pravila prije nego možete pokrenuti vaše VPN veze.

Ne možete aktivirati (ili deaktivirati) paketna pravila kada imate VPN veze u izvođenju na vašem sistemu. Zato, prije nego aktivirate vaša VPN pravila filtriranja, osigurajte da nema njima pridruženih aktivnih veza.

Ako ste vaše VPN veze kreirali pomoću Čarobnjaka za nove veze, možete izabrati da se pridružena pravila aktiviraju automatski za vas. Budite svjesni da, ako ima drugih paketnih pravila na bilo kojem od sučelja koja specificirate, pravila filtriranja VPN politike će ih zamijeniti.

Ako odlučite aktivirati vaša VPN generirana pravila koristeći Editor paketnih pravila, slijedite ove korake:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje paketnih pravila**.

3. Izaberite želite li aktivirati samo VPN generirana pravila, samo izabranu datoteku ili oboje, VPN generirana pravila i izabranu datoteku. Ovo posljednje biste mogli izabrati ako, na primjer, imate svakovrsna PERMIT i DENY pravila koja želite nametnuti sučelju kao dodatak VPN generiranim pravilima.
4. Izaberite sučelje na kojem želite aktivaciju pravila. Možete izabrati aktivaciju na određenom sučelju, na point-to-point identifikatoru ili na svim sučeljima i svim point-to-point identifikatorima.
5. Kliknite na **OK** u kućici dijaloga da potvrdite kako želite provjeriti i aktivirati pravila na sučelju ili sučeljima koje ste naveli. Nakon što kliknete OK, sistem provjerava pravila od sintaktičkih i semantičkih pogrešaka i daje izvještaj o rezultatima u prozoru za poruke na dnu editora. Za poruke o greškama koje se odnose na određenu datoteku ili broj linije, možete desno kliknuti na grešku i izabrati **Idi na liniju** da osvijetlite grešku u datoteci.

Nakon aktivacije pravila filtera, možete pokrenuti VPN vezu.

Srodni koncepti

"Konfiguriranje VPN paketnih pravila" na stranici 48
Ako kreirate vezu po prvi puta, dozvolite VPN-u da automatski generira pravila VPN paketa umjesto vas. To možete napraviti ili korištenjem Čarobnjaka za novu vezu ili stranice VPN svojstava za konfiguriranje vaše veze.

Srodni zadaci

"Konfiguriranje sigurne VPN veze" na stranici 47
Nakon što ste konfigurirali politike sigurnosti za vašu vezu morate konfigurirati sigurnu vezu.

"Definiranje sučelja za VPN pravila filtera" na stranici 52
Nakon što konfigurirate vaša VPN paketna pravila i bilo koja druga pravila koja trebate da omogućite vašu VPN vezu, morate definirati sučelje na koje se ta pravila primjenjuju.

"Pokretanje VPN veze" na stranici 54
Dovršite ovaj zadatak da pokrenete veze koje ćete započeti lokalno.

Konfiguriranje povjerljivog toka podataka

Ako je vaša politika podataka konfigurirana za tunelski način, možete koristiti povjerljivi tok podataka (TFC), da sakrijete stvarnu dužinu paketa podataka prenesenih preko VPN veze.

TFC dodaje dodatno punjenje paketima koji se šalju i šalje dummy pakete s različitim dužinama u nasumičnim intervalima kako bi se sakrila stvarna veličina paketa. TFC koristite za dodatnu sigurnost protiv napadača koji mogu pogoditi prema veličini paketa pogoditi koji se podaci šalju. Omogućavanjem TFC-a, dobivate veću sigurnost, ali uz trošak na performansama sistema. Zato, trebate testirati performanse sistema prije i poslije omogućavanja TFC-a na VPN vezi. TFC ne dogovara IKE i korisnik može samo omogućiti TFC kad ga podržavaju oba sistema.

Za omogućavanje TFC-a na VPN vezi slijedite ove korake:

1. U System i Navigator, proširite vaš poslužitelj **> Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze → Sve veze**.
2. Desno kliknite na vezu kojoj želite omogućiti TFC i izaberite **Svojstva**.
3. Na kartici **Općenito** izaberite **Koristi povjerljivost toka prometa (TFC) u Tunel načinu**

Konfiguriranje proširenog rednog broja

Prošireni redni broj (ESN) možete koristiti da povećate količinu prijenosa podataka za VPN vezu.

Ako koristite AH protokol ili ESP protokol i algoritam šifriranja je AES, možda ćete omogućiti ESN. ESN omogućava prijenos velikog obujma podataka pri visokim brzinama bez ponovnog kriptiranja. VPN veza koristi 64-bit redne brojeve umjesto 32-bit brojeva preko IPSec. Korištenje 64-bit rednih brojeva omogućava više vremena prije ponovnog kriptiranja, što sprečava iscrpljenje rednih brojeva i smanjuje korištenje sistemskih resursa.

Za omogućavanje ESN za VPN vezu slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje**
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Svojstva**.

3. Na kartici **Općenito** izaberite **Koristi proširen redni broj (ESN)**.

Pokretanje VPN veze

Dovršite ovaj zadatak da pokrenete veze koje ćete započeti lokalno.

Ove upute pretpostavljaju da ste ispravno konfigurirali vašu VPN vezu. Slijedite sljedeće korake da pokrenete vašu VPN vezu:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Ako VPN poslužitelj nije pokrenut, desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Pokreni**.
3. Osigurajte da su aktivirana paketna pravila.
4. Proširite **Virtualno privatno umrežavanje → Sigurne veze**.
5. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
6. Desno kliknite na vezu koju želite pokrenuti i izaberite **Pokreni**. Da pokrenete više veza, izaberite svaku vezu koju želite pokrenuti, desno kliknite i izaberite **Pokreni**.

Srodni zadaci

"Aktiviranje VPN paketnih pravila" na stranici 52
Morate aktivirati VPN paketna pravila prije nego možete pokrenuti vaše VPN veze.

"Kako započeti s VPN rješavanjem problema" na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Upravljanje VPN-a

Možete koristiti VPN sučelje u System i Navigator da rukujete svim vašim zadacima VPN upravljanja kao što je zaustavljanje veze i gledanje atributa veze.

VPN sučelje koristite System i Navigator za obavljanje zadataka upravljanja, uključujući:

Postavljanje default atributa za vaše veze

Default vrijednosti ispunjavaju panele koje koristite za kreiranje novih politika i veza. Možete postaviti default vrijednosti za razine sigurnosti, upravljanje sesijom ključa, životne vjekove ključeva i životne vjekove veza.

Default sigurnosne vrijednosti zaposjedaju razna polja prilikom inicijalnog kreiranja novih VPN objekata.

Za postavku default vrijednosti za vaše VPN veze, slijedite ove korake:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite **Virtualno privatno umrežavanje** i izaberite **Defaulti**.
3. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
4. Kliknite **OK** nakon dovršenja lista papira svakog svojstva.

Resetiranje veza u stanju greške

Resetiranje veza s greškom vraća ih u stanje mirovanja.

Da osvježite vezu koja je u stanju greške, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na vezu koju želite resetirati i izaberite **Resetiraj**. Ovo resetira vezu u stanje 'u mirovanju'. Da resetirate više veza koje su u stanju greške, izaberite svaku vezu koju želite resetirati, desno kliknite i izaberite **Resetiraj**.

Gledanje informacija o grešci

Dovršite ovaj zadatak da vam pomogne odrediti kako vaša veza uzrokuje grešku.

Za gledanje informacija o vezama u stanju greške, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na vezu s greškom koju želite pogledati i izaberite **Informacije o greški**.

Srodni zadaci

"Kako započeti s VPN rješavanjem problema" na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Gledanje atributa aktivnih veza

Ispunite ovaj zadatak da provjerite status i ostale atribute vaših aktivnih veza.

Da pogledate trenutne atribute aktivne veze ili veze na-zahtjev, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na aktivnu on-demand vezu koju želite pogledati i izaberite **Svojstva**.
4. Otiđite na stranicu **Trenutni atributi** da pogledate atribute veze.

Također, možete pogledati atribute svih veza s prozora System i Navigator. Po defaultu, jedini atributi koji su prikazani su Status, Opis i Tip veze. Možete promijeniti koji se podaci prikazuju, slijedeći ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Iz izbornika **Objekti** izaberite **Stupci**. Ovo otvara kućicu dijaloga koja vam omogućava izbor atributa koje želite prikazati u prozoru System i Navigator.

Imajte da umu da kada mijenjate stupce za pogled, promjene nisu specifične za određenog korisnika ili PC, već za cijeli sistem.

Srodni koncepti

"Uobičajene poruke o greški VPN Upravitelja veze" na stranici 69
VPN Upravitelj veze zapisuje dvije poruke u QTOVMAN dnevnik posla kada dođe do greške s VPN povezivanjem.

Gledanje traga VPN poslužitelja

Omogućava konfiguriranje, pokretanje, zaustavljanje i pregled VPN upravitelja veze, tragovi poslužitelja VPN upravitelja ključa. Ovo je slično korištenju TRCTCPAPP *VPN naredbe iz znakovnog sučelja osim što možete gledati praćenje dok je veza aktivna.

Da pogledate praćenje VPN poslužitelja, slijedite ove korake:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite **Virtualno privatno umrežavanje**, izaberite **Dijagnostički alati** i zatim **Trag poslužitelja**.

Da navedete koji tip praćenja želite da generiraju VPN Upravitelj ključa i VPN Upravitelj veze, slijedite ove korake:

1. Iz prozora **Trag Virtualnog privatnog umrežavanja**, kliknite na  (Opcije).

2. Na stranici **Upravitelj veze** navedite koji tip praćenja želite da izvodi poslužitelj Upravitelj veze.
3. Na stranici **Upravitelj ključa**, navedite koji tip treba izvoditi poslužitelj Upravitelja ključa za praćenje.
4. Kliknite **Pomoć** ako imate pitanja kako dovršiti stranicu ili bilo koja od tih polja.
5. Kliknite **OK** za spremanje promjena.
6. Kliknite  (Pokreni) da pokrenete praćenje. Povremeno kliknite na  (Osvježavanje) da pogledate zadnje informacije praćenja.

Gledanje dnevnika posla VPN poslužitelja

Slijedite ove upute da pogledate dnevnike poslova za Upravitelja VPN ključa i Upravitelja VPN veze.

Za pogled na trenutne dnevnike poslova ili VPN Upravitelja ključeva ili VPN Upravitelja veza, slijedite ove korake:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Alati za dijagnostiku**, a zatim izaberite dnevnik posla koji želite pogledati.

Gledanje atributa sigurnosnih asocijacija

Dovršite ovaj zadatak da prikažete atribute Sigurnosnih asocijacija (SA) koji su pridruženi omogućenoj vezi.

Da pogledate atribute sigurnosnih asocijacija (SA) koje su pridružene omogućenoj vezi. Da to napravite, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na odgovarajuću aktivnu vezu i izaberite **Sigurnosne asocijacije**. Rezultirajući prozor omogućava pregled svojstava svake SA koja je pridružena navedenoj vezi.

Zaustavljanje VPN veze

Dovršite ovaj zadatak da zaustavite aktivne veze.

Da zaustavite aktivnu vezu ili vezu na-zahtjev, slijedite ove korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na vezu koju želite zaustaviti i izaberite **Zaustavi**. Da zaustavite više veza, izaberite svaku vezu koju želite zaustaviti, desno kliknite i izaberite **Zaustavi**.

Brisanje objekata VPN konfiguracije

Prije nego obrišete objekt VPN konfiguracije iz baze podataka VPN politika, uvjerite se da razumijete kako to utječe na ostale VPN veze i grupe veza.

Ako ste sigurni da trebate brisati VPN vezu iz baze podataka VPN politika, izvedite sljedeće korake:

1. U System i Navigator, proširite **sistem → Mreža → IP politike → Virtualno privatno umrežavanje → Sigurne veze**
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na vezu koju želite obrisati i izaberite **Brisanje**.

Rješavanje problema VPN-a

Koristite sljedeće načine rješavanja problema da riješite neke od osnovnih problema koje možete iskusiti kod konfiguracije VPN veze.

VPN je kompleksna i brzo mijenjajuća tehnologija koja zahtijeva barem osnovno znanje standardnih IPSec tehnologija. Morate također biti upoznati s pravilima IP paketa, jer VPN zahtijeva nekoliko pravila filtera za ispravan rad. Zbog ove kompleksnosti ćete možda, s vremena na vrijeme, iskusiti neprilike s vašim VPN vezama. Rješavanje problema na vašem VPN-u nije uvijek lagan zadatak. Morate razumjeti vaš sistem i vaše mrežne okoline, kao i komponente koje koristite za njihovo upravljanje. Sljedeća poglavlja sadrže savjete kako riješiti razne probleme na koje možete naići za vrijeme korištenja VPN-a:

Kako započeti s VPN rješavanjem problema

Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Nekoliko je načina za početak analiziranja VPN problema:

1. Uvijek provjerite da ste primijenili zadnje Privremene popravke za program (PTF).
2. Osigurajte da odgovarate minimalnim zahtjevima postavljanja VPN-a.
3. Pregledajte sve poruke o grešci koje se nalaze u prozoru Informacije o grešci ili u dnevnicima poslova VPN poslužitelja za lokalne i udaljene sisteme. Zapravo, kada uklanjate pogreške za problem VPN veze, često je potrebno gledati na oba kraja veze. Nadalje, trebate uzeti u obzir da postoje četiri adrese koje morate provjeriti: lokalne i udaljene krajnje točke za vezu (što su adrese gdje je IPSec primijenjen na IP pakete) i lokalne i udaljene krajnje točke za podatke (što su izvorne i odredišne adrese IP paketa).
4. Ako vam poruke o greškama ne daju dovoljno informacija za rješavanje problema, provjerite dnevnik IP filtera.
5. Praćenje komunikacija na sistemu još je jedno mjesto gdje možete pronaći općenite informacije o tome da li lokalni sistem prima ili šalje zahtjeve za vezom.
6. Naredba Praćenje TCP aplikacije (TRCTCPAPP) daje još jedan način za izoliranje problema. Tipično, IBM Servis koristi TRCTCPAPP za dobivanje praćenja izlaza u svrhu analize problema s vezom.

Srodni koncepti

"Zahtjevi za VPN postav" na stranici 40
Da bi VPN veza ispravno funkcionirala na vašim sistemima i s mrežnim klijentima, morate zadovoljiti minimum zahtjeva

"Rješavanje VPN-a s VPN dnevnicima posla" na stranici 68
Kada naiđete na probleme s vašim VPN vezama, uvijek je preporučljivo da analizirate dnevnike poslova. Zapravo, nekoliko je dnevnika poslova koji sadrže poruke greške i druge informacije koje se odnose na VPN okolinu.

"Rješavanje problema VPN-a s praćenjem komunikacija" na stranici 73
IBM i5/OS osigurava sposobnost praćenja podataka komunikacijske linije, kao što su sučelja Mreže lokalnog područja (LAN) ili Mreže širokog područja (WAN). Prosječan korisnik možda neće shvatiti cijeli sadržaj podataka praćenja. Međutim, možete koristiti unose praćenja da odredite da li se dogodila razmjena podataka između lokalnih i udaljenih sistema.

Srodni zadaci

"Gledanje informacija o grešci" na stranici 55
Dovršite ovaj zadatak da vam pomogne odrediti kako vaša veza uzrokuje grešku.

"Rješavanje problema VPN-a s QIPFILTER dnevnikom" na stranici 63
Ove informacije pregledajte kako biste naučili o pravilima VPN filtera.

"Pokretanje VPN veze" na stranici 54
Dovršite ovaj zadatak da pokrenete veze koje ćete započeti lokalno.

Ostale stvari za provjeru

Ako se greška dešava nakon što postavite vezu, a niste sigurni gdje na mreži je došlo do greške, pokušajte smanjiti kompleksnost vaše okoline. Na primjer, umjesto istraživanja svih dijelova VPN veze odjednom, započnite sa samom IP vezom. Sljedeći popis vam daje neke osnovne upute o tome kako započeti analizu VPN problema, od najjednostavnije IP veze do složenije VPN veze:

1. Započnite s IP konfiguracijom između lokalnog i udaljenog hosta. Uklonite bilo kakve IP filtere na sučelju koje oba sistema, lokalni i udaljeni, koriste za komuniciranje. Možete li napraviti PING s lokalnog na udaljeni host?

   Bilješka: Ne zaboravite prompt kod naredbe PING; unesite adresu udaljenog sistema i koristite PF10 za dodatne parametre i unesite lokalnu IP adresu. Ovo je od posebne važnosti kada imate višestruka fizička ili logička sučelja. To osigurava da su ispravne adrese smještene u PING pakete.

   Ako odgovorite **da**, tada nastavite s korakom 2. Ako odgovorite **ne**, tada provjerite vašu IP konfiguraciju, status sučelja i unose usmjeravanja. Ako je konfiguracija ispravna, koristite praćenje veze za provjeru, na primjer, da je PING zahtjev napustio sistem. Ako pošaljete PING zahtjev, ali ne primite odgovor, problem je najvjerojatnije u mreži ili udaljenom sistemu.

   Bilješka: Mogu postojati posredni usmjerivači ili vatrozid koji izvode filtriranje IP paketa i mogu postojati PING paketi filtriranja. PING se uobičajeno bazira na ICMP protokolu. Ako je PING uspješan, znate da imate povezanost. Ako je PING neuspješan, znate samo da PING nije uspio. Možda ćete htjeti probati druge IP protokole između dva sistema, kao što je Telnet ili FTP za provjeru povezanosti.
2. Provjerite pravila filtriranja za VPN i osigurajte da su aktivirana. Da li je pokretanje filtriranja uspješno? Ako odgovorite **da**, nastavite s korakom 3. Ako odgovorite **ne**, provjerite poruke o grešci u prozoru Pravila paketa u System i Navigatoru. Osigurajte da pravila filtriranja ne navode Prijevod mrežne adrese (NAT) za bilo koji VPN promet.
3. Pokrenite VPN vezu. Da li je pokretanje veze uspješno? Ako odgovorite **da**, tada nastavite s korakom 4. Ako odgovorite **ne**, tada provjerite od grešaka dnevnik posla QTOVMAN i dnevnike poslova QTOKVPNIKE. Kada koristite VPN, vaš Dobavljač Internet usluge (ISP) i svaki sigurnosni prilaz u vašoj mreži mora podržavati protokole Zaglavlje za provjeru autentičnosti (AH) i Sažimanje tereta sigurnosti (ESP). Da li ćete izabrati korištenje AH ili ESP protokola ovisi o planovima koje definirate za vašu VPN vezu.
4. Da li možete aktivirati korisničku sesiju preko VPN veze? Ako odgovorite **da**, tada VPN veza radi kao što je potrebno. Ako odgovorite **ne**, tada provjerite pravila paketa i VPN grupe dinamičkog ključa te veze za definicije filtera koji ne dozvoljavaju korisnički promet koji želite.

Najčešće VPN konfiguracijske greške i kako ih popraviti

Koristite ove informacije da pogledate uobičajene VPN poruke greške i naučite o njihovim mogućim rješenjima.

Bilješka: Pri konfiguriranju VPN-a, stvarno kreirate nekoliko različitih konfiguracijskih objekata, a svaki od VPN zahtijeva omogućavanje veze. Ako se radi o VPN GUI-u, ovi objekti su: Politike IP sigurnosti i Sigurne veze. Dakle, kada se ove informacije odnose na objekt, odnose se na jedan ili više od ovih dijelova VPN-a.

VPN poruka greške: TCP5B28

Kada pokušate aktivirati pravila filtriranja na sučelje, dobivate ovu poruku: TCP5B28 CONNECTION_DEFINITION povreda poretka

Simptom:

Kada pokušate aktivirati pravila filtriranja na određeno sučelje, dobivate ovu poruku greške:

```
TCP5B28: CONNECTION_DEFINITION prekršaj naredbe
```

Moguće rješenje:

Pravila filtriranja koja ste pokušali aktivirati sadrže definicije veze poredane različito nego u prethodno aktiviranom skupu pravila. Najlakši način za rješavanje ove greške je aktiviranje datoteke s pravilima na **svim sučeljima** umjesto na određenom sučelju.

VPN poruka greške: Stavka nije pronađena

Kada desno kliknete na VPN objekt i izaberete ili **Svojstva** ili **Brisanje**, dobivate poruku koja kaže, **Stavka nije pronađena**.

Simptom:

Pri desnom kliku na objekt u prozoru Virtualno privatno umrežavanje i izborom **Svojstva** ili **Brisanje**, pojavljuje se sljedeća poruka:

Moguće rješenje:

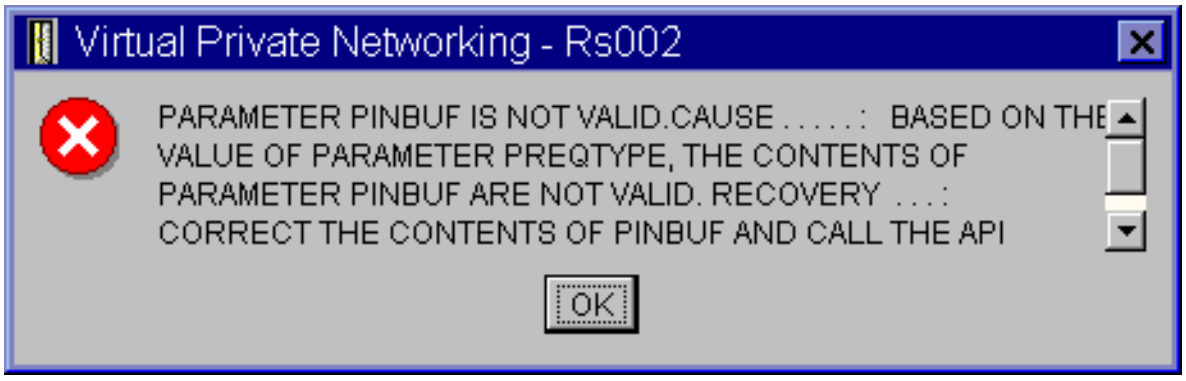
- Možda ćete trebati obrisati objekt ili ga preimenovati, a još niste osvježili prozor. Kao posljedica, objekt se još pojavljuje na prozoru Virtualno privatno umrežavanje. Da potvrdite da se radi o ovom slučaju, iz izbornika **Pogled** izaberite **Osvježi**. Ako se objekt još uvijek pojavljuje u prozoru Virtualno privatno umrežavanje, prijeđite na sljedeću stavku na ovom popisu.
- Nakon konfiguracije svojstava za objekt, možda je došlo do komunikacijske greške između VPN poslužitelja i vašeg sistema. Mnogi objekti koji se pojavljuju u VPN prozoru odnose se na više od jednog objekta u bazi podataka VPN politika. To znači da komunikacijske greške mogu uzrokovati da se neki od objekata u bazi podataka mogu nastaviti odnositi na objekt u VPN-u. Uvijek kada kreirate ili ažurirate objekt desit će se greška kada se desi gubitak sinkronizacije. Jedini način da se riješi ovaj problem je da izaberete **OK** na prozoru za greške. To lansira list sa svojstvima objekta koji javlja grešku. Samo polje imena na listu sa svojstvima u sebi nosi vrijednost. Sve ostalo je prazno (ili sadrži default vrijednosti). Upišite ispravne atribute objekta i izaberite **OK** da spremite vaše promjene.
- Slična greška se dešava kada pokušate obrisati objekt. Da popravite ovaj problem, ispunite list s praznim vrijednostima svojstava koji se otvara kada kliknete **OK** na poruci greške. Ovo ažurira svaku vezu na bazu podataka VPN politika koja je bila izgubljena. Sada možete obrisati objekt.

VPN poruka greške: PARAMETER PINBUF IS NOT VALID

Pri pokušaju pokretanja veze, dobit ćete poruku koja kaže, **PARAMETAR PINBUF NIJE VAŽEĆI...**

Simptom:

Pri pokušaju pokretanja veze, dobivate poruku sličnu ovoj:



Moguće rješenje:

Do ovoga dolazi kada je vaš sistem postavljen da koristi određene lokalizacije na koje se mala slova ne mapiraju ispravno. Da popravite ovu grešku ili osigurajte da svi objekti koriste samo velika slova ili promijenite lokalizaciju sistema.

Poruka VPN greške: Stavka nije pronađena, Udaljeni poslužitelj ključa...

Kada izaberete **Svojstva** za vezu dinamičkog ključa, dobivate grešku koja kaže da poslužitelj ne može pronaći udaljeni poslužitelj ključa koji ste naveli.

Simptom:

Izborom **Svojstva** za vezu dinamičkog ključa, pojavljuje se poruka slična ovoj:

Moguće rješenje:

Ovo se događa kada kreirate vezu s određenim identifikatorom za udaljeni poslužitelj ključa, a zatim je udaljeni poslužitelj ključa uklonjen iz svoje grupe dinamičkog ključa. Da popravite ovu grešku, kliknite **OK** na poruci greške. Ovo otvara list za svojstva za vezu dinamičkog ključa koja je u statusu greške. Od tamo možete ili dodati udaljeni poslužitelj ključa natrag u grupu dinamičkog ključa ili izabrati drugi identifikator za udaljeni poslužitelj ključa. Kliknite **OK** na listu za svojstva da spremite vaše promjene.

VPN poruka greške: Nije moguće ažurirati objekt

Kada izaberete **OK** na listu sa svojstvima za grupu dinamičkog ključa ili ručnu vezu, dobivate poruku koja vam kaže da sistem ne može ažurirati objekt.

Simptom:

Kada izaberete **OK** na listi sa svojstvima grupe dinamičkog ključa ili ručne veze, dobivate sljedeću poruku:

Moguće rješenje:

Greška se događa kada aktivna veza koristi objekt na kojem pokušavate napraviti promjene. Ne možete raditi promjene na objektu unutar aktivne veze. Da napravite promjene na objektu, identificirajte prikladnu aktivnu vezu, zatim desno kliknite na nju i izaberite **Zaustavljanje** iz rezultirajućeg kontekstnog izbornika.

VPN poruka greške: Nije moguće šifriranje ključa...

dobivate poruku koja kaže da sistem ne može šifrirati vaše ključeve zato jer vrijednost QRETSVRSEC mora biti postavljena na 1.

Simptom:

Pojavljuje se sljedeća poruka greške:

Moguće rješenje:

QRETSVRSEC je sistemska vrijednost koja pokazuje da li vaš sistem može pohraniti šifrirane ključeve. Ako je ova vrijednost postavljena na 0, tada unaprijed podijeljeni ključevi i ključevi za algoritme u ručnoj vezi ne mogu biti pohranjeni u bazi podataka VPN politika. Da riješite ovaj problem, koristite 5250 sesiju za emulaciju na vašem sistemu. Upišite wrksysval u redu za naredbe i pritisnite **Enter**. Potražite QRETSVRSEC na popisu i pokraj njega upišite 2 (promjena). Na sljedećem panelu upišite 1 i pritisnite **Enter**.

Srodni koncepti

"VPN greška: Svi ključevi su praznine"
Kada gledate svojstva ručne veze, svi unaprijed podijeljeni ključevi i ključevi algoritama za vezu su praznine.

VPN poruka greške: CPF9821

Kada pokušate proširiti ili otvoriti spremnik IP politika u System i Navigator, pojavljuje se poruka CPF9821- nije ovlašten da programira QTFRPRS u QSYS knjižnici.

Simptom:

Kada pokušate proširiti spremnik IP politika u System i Navigator, pojavljuje se poruka CPF9821- nije ovlašten da programira QTFRPRS u QSYS knjižnici.

Moguće rješenje:

Možda nećete imati potrebno ovlaštenje za primanje trenutnog statusa Paketnih pravila ili VPN upravitelja mreže. Osigurajte da imate *IOSYSCFG ovlaštenje za dohvaćanje pristupa funkcijama Paketnih pravila u System i Navigator.

VPN greška: Svi ključevi su praznine

Kada gledate svojstva ručne veze, svi unaprijed podijeljeni ključevi i ključevi algoritama za vezu su praznine.

Simptom:

Svi unaprijed podijeljeni ključevi i ključevi algoritma za ručne veze su praznine.

Moguće rješenje:

Ovo se događa kad je sistemska vrijednost QRETSVRSEC postavljena na 0. Postavljanjem ove sistemske vrijednosti na 0 briše sve ključeve u bazi podataka VPN politika. Da riješite ovaj problem, morate postaviti sistemsku vrijednost na 1 i zatim ponovo unijeti sve ključeve. Za više informacija kako to učiniti, uputite se na poruku o grešci: Nije moguće šifriranje ključeva.

Srodni koncepti

"VPN poruka greške: Nije moguće šifriranje ključa..." na stranici 60
dobivate poruku koja kaže da sistem ne može šifrirati vaše ključeve zato jer vrijednost QRETSVRSEC mora biti postavljena na 1.

VPN greška: javlja se prijava za drugi sistem kod korištenja Paketnih pravila

Pri prvom korištenju sučelja Pravila paketa u System i Navigator, prikazuje se prikaz prijave za drugi sistem od trenutnog.

Simptom:

Prvi put kada koristite Paketna pravila, javlja se ekran za prijavu za sistem različit od trenutnog.

Moguće rješenje:

Paketna pravila koriste univerzalni kod za pohranu pravila za paketnu sigurnost u integriranom sistemu datoteka. Dodatna prijava omogućava System i Access za Windows dobivanje odgovarajuće tablice konverzije za Unicode. Ovo će se desiti samo jednom.

VPN greška: Status veze je praznina u System i Navigator prozoru

Veza nema vrijednost u stupcu **Status** u prozoru System i Navigator.

Simptom:

Veza nema vrijednost u stupcu **Status** u prozoru System i Navigator.

Moguće rješenje:

Prazna vrijednost statusa označava da je veza usred pokretanja. To znači, još nije u izvođenju, ali još nije došlo ni do greške. Kada osvježite prozor, veza će ili prikazati status Greška, Omogućeno, Na-zahtjev ili U mirovanju.

VPN greška: Veza ima status omogućeno nakon što ste ju zaustavili

Nakon zaustavljanja veze, System i Navigator prozor pokazuje da je veza i dalje omogućena.

Simptom:

Nakon zaustavljanja veze, System i Navigator prozor pokazuje da je veza i dalje omogućena.

Moguće rješenje:

Ovo se obično događa jer nemate osvježen System i Navigator prozor. Takav neosvježeni prozor sadrži zastarjele informacije. Da ovo popravite, iz izbornika **Pogled** izaberite **Osvježi** .

VPN greška: 3DES nije izbor za šifriranje

Kada radite s pretvorbom IKE politike, pretvorbom politike podataka ili ručnim povezivanjem, algoritam za 3DES šifriranje nije izbor.

Simptom:

Kada radite s pretvorbom IKE politike, pretvorbom politike podataka ili ručnim povezivanjem, algoritam za 3DES šifriranje nije izbor.

Moguće rješenje:

Najčešće imate samo proizvod Dobavljača kriptografskog pristupa (5722-AC2) instaliran na vašem sistemu, a ne Dobavljača kriptografskog pristupa (5722-AC3). Dobavljač kriptografskog pristupa (5722-AC2) dopušta samo algoritam šifriranja Standardno šifriranje podataka (DES), zbog ograničenja dužina ključa. Dobavljač kriptografskog pristupa (5722-AC2) i (5722-AC3) više nisu potrebni za omogućavanje šifriranja podataka na sistemima koji izvode i5/OS V5R4 ili kasniji.

VPN greška: U System i Navigator prozoru prikazani su neočekivani stupci.

Postav stupaca koje želite prikazati u System i Navigator prozoru za VPN veze; nakon toga, prikazuju se drugačiji stupci.

Simptom:

Postavljate stupce koje želite prikazati u System i Navigator prozoru za VPN veze; nakon toga, prikazuju se drugačiji stupci.

Moguće rješenje:

Kada mijenjate stupce za pogled promjene nisu specifične za određenog korisnika ili PC, već za cijeli sistem. Stoga, kada netko drugi mijenja stupce u prozoru, promjene utječu na sve koji gledaju veze na tom sistemu.

VPN greška: Neuspjeh deaktiviranja aktivnih pravila filtriranja

Kada pokušate deaktivirati trenutni skup pravila filtriranja, javlja se poruka Neuspjeh deaktiviranja aktivnih pravila u prozoru za rezultate.

Simptom:

Kada pokušate deaktivirati trenutni skup pravila filtriranja, javlja se poruka Neuspjeh deaktiviranja aktivnih pravila u prozoru za rezultate.

Moguće rješenje:

Ova poruka greške najčešće znači da postoji barem jedna aktivna VPN veza. Morate zaustaviti svaku od veza koja ima status omogućeno. Da to napravite, desno kliknite svaku od aktivnih veza i izaberite **Zaustavi**. Sada možete deaktivirati pravila filtera.

VPN greška: Promijenila se grupa veze ključa za ovu vezu

Kada kreirate vezu dinamičkog ključa, navodite grupu dinamičkog ključa i identifikator za udaljeni poslužitelj ključa. Kasnije, kada gledate svojstva srodnog objekta veze, stranica Općenito lista za svojstva prikazuje isti identifikator udaljenog poslužitelja ključa, ali različitu grupu dinamičkog ključa.

Simptom:

Kada kreirate vezu dinamičkog ključa, navodite grupu dinamičkog ključa i identifikator za udaljeni poslužitelj ključa. Kasnije, kada izaberete **Svojstva** na srodnom objektu veze, stranica **Općenito** lista za svojstva prikazuje isti identifikator poslužitelja udaljenog ključa, ali različitu grupu dinamičkog ključa.

Moguće rješenje:

Identifikator je jedina informacija pohranjena u bazi podataka VPN politika koja se odnosi na udaljeni poslužitelj ključa za vezu dinamičkog ključa. Kada VPN potraži politiku za udaljeni poslužitelj ključa, najprije traži prvu grupu dinamičkog ključa koja u sebi ima identifikator tog udaljenog poslužitelja ključa. Zato, kada gledate svojstva jedne od ovih veza, ona koristi istu grupu dinamičkog ključa koju je VPN pronašao. Ako ne želite pridružiti grupu dinamičkog ključa tom udaljenom poslužitelju ključa, možete napraviti jedno od sljedećeg:

1. Uklonite udaljeni poslužitelj ključa iz grupe dinamičkog ključa.
2. Proširite **Po grupi** u lijevom oknu VPN sučelja i izaberite i povucite grupu dinamičkog ključa koju želite na vrh tablice u desnom oknu. Ovo osigurava da VPN provjerava prvo ovu grupu dinamičkog ključa za udaljeni poslužitelj ključa.

Rješavanje problema VPN-a s QIPFILTER dnevnikom

Ove informacije pregledajte kako biste naučili o pravilima VPN filtera.

QIPFILTER dnevnik se nalazi u knjižnici QUSRSYS i sadrži informacije o skupovima pravila filtriranja, kao i informacije o tome da li je IP datogram bio dozvoljen ili odbijen. Zapisivanje se izvodi na osnovu opcije za vođenje dnevnika koju ste specificirali u vašim pravilima filtriranja.

Srodni zadaci

"Kako započeti s VPN rješavanjem problema" na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Omogućavanje QIPFILTER dnevnika

Za aktivaciju QIPFILTER dnevnika koristite editor Paketa pravila u System i Navigator.

Morate omogućiti funkciju zapisivanja za svako individualno pravilo filtera. Ne postoji funkcija koja dozvoljava zapisivanje za sve IP datograme koji ulaze ili izlaze iz sistema.

Bilješka: Za omogućavanje QIPFILTER dnevnika, morate deaktivirati filtere.

Sljedeći koraci opisuju kako omogućiti vođenje dnevnika za određeno pravilo filtriranja:

1. U System i Navigator, proširite vaš **sistem → Mreža → IP politike**.
2. Desno kliknite na **Pravila paketa** i izaberite **Konfiguracija**. Ovo prikazuje sučelje Pravila paketa.
3. Otvorite postojeću datoteku za pravila filtriranja.
4. Dvostruko kliknite pravilo filtriranja za koje želite voditi dnevnik.

5. Na stranici **Općenito**, izaberite **FULL** u polju **Vođenje dnevnika** kao što je u kućici dijaloga gore. Ovo omogućuje zapisivanje za ovo određeno pravilo filtriranja.
6. Kliknite **OK**.
7. Spremite i aktivirajte promijenjenu datoteku za pravila filtriranja.

Ako se IP datogram podudara s definicijama pravila filtriranja, radi se unos u QIPFILTER dnevnik.

Upotreba QIPFILTER dnevnika

i5/OS automatski kreira dnevnik čim prvi put aktivirate filtriranje IP paketa.

Da u dnevniku pogledate detalje specifične za unos, možete na ekranu prikazati unose u dnevnik ili možete koristiti izlaznu datoteku. Kopiranjem unosa u dnevnik u izlaznu datoteku lako možete pogledati unose koristeći uslužne programe za upit, kao što su Query/400 ili SQL. Također, možete pisati vaše vlastite HLL programe da obradite unose u izlaznim datotekama.

Slijedi primjer naredbe Prikaz Dnevnika (DSPJRN):

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

Koristite sljedeće korake za kopiranje unosa QIPFILTER dnevnika u izlaznu datoteku:

1. Kreirajte kopiju izlazne datoteke QSYS/QATOFIPF dobavljene od sistema u korisničkoj knjižnici, korištenjem naredbe Kreiraj duplikat objekta (CRTDUPOBJ). Slijedi primjer naredbe CRTDUPOBJ:

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

2. Koristite naredbu Prikaži dnevnik (DSPJRN) da kopirate unose iz dnevnika QUSRSYS/QIPFILTER u izlaznu datoteku koju ste kreirali u prethodnom koraku.

Ako pokušate kopirati DSPJRN u izlaznu datoteku koja ne postoji, sistem kreira tu datoteku umjesto vas, ali ova datoteka ne sadrži ispravne opise polja.

Bilješka: Dnevnik QIPFILTER journal sadrži samo dopuštene i nedopuštene unose pravila filtera gdje je opcija vođenja dnevnika postavljena na FULL. Na primjer ako podesite samo PERMIT filter pravilo, IP datogramima kojima to nije izričito dozvoljeno su odbijeni. Za ove odbijene datograme ne dodaje se nikakav unos u dnevnik. Za analizu problema možete dodati pravilo filtriranja koje izričito zabranjuje sav drugi promet i izvodi FULL vođenje dnevnika. Tada ćete dobiti DENY unose u dnevnik za sve IP datograme koji su odbijeni. Zbog performanse nije preporučljivo da omogućite vođenje dnevnika za sva pravila filtriranja. Jednom kada su vaši skupovi filtera testirani, smanjite vođenje dnevnika samo na koristan podskup unosa.

Srodni koncepti

"Polja QIPFILTER dnevnika"
Pregledajte sljedeću tablicu koja opisuje polja u QIPFILTER izlaznoj datoteci

Polja QIPFILTER dnevnika

Pregledajte sljedeću tablicu koja opisuje polja u QIPFILTER izlaznoj datoteci

Ime polja	Dužina polja	Numerički	Opis	Komentari
TFENTL	5	Y	Dužina unosa	
TFSEQN	10	Y	Redni broj	
TFCODE	1	N	Kod dnevnika	Uvijek M
TFENTT	2	N	Tip unosa	Uvijek TF
TFTIME	26	N	SAA timestamp	
TFJOB	10	N	Ime posla	
TFUSER	10	N	Profil korisnika	

Ime polja	Dužina polja	Numerički	Opis	Komentari
TFNBR	6	Y	Broj posla	
TFPGM	10	N	Ime programa	
TFRES1	51	N	Rezervirano	
TFUSPF	10	N	Korisnik	
TFSYMN	8	N	Ime sistema	
TFRES2	20	N	Rezervirano	
TFRESA	50	N	Rezervirano	
TFLINE	10	N	Opis linije	*ALL ako je TFREVT U* , Praznina ako je TFREVT L*, Ime linije ako je TFREVT L
TFREVT	2	N	Događaj pravila	L* ili L kada su pravila učitana. U* kada pravila odstranjena, A za akciju filtriranja
TFPDIR	1	N	Smjer IP Paketa	O je izlazni, I je ulazni
TFRNUM	5	N	Broj pravila	Odnosi se na broj pravila u datoteci aktivnih pravila
TFACT	6	N	Poduzeta akcija filtriranja	PERMIT, DENY ili IPSEC
TFPROT	4	N	Protokol prijenosa	1 je ICMP 6 je TCP 17 je UDP 50 je ESP 51 je AH
TFSRCA	15	N	IP adresa izvora	
TFSRCP	5	N	Port izvora	Smeće ako TFPROT= 1 (ICMP)
TFDSTA	15	N	IP adresa odredišta	
TFDSTP	5	N	Port odredišta	Smeće ako TFPROT= 1 (ICMP)
TFTEXT	76	N	Dodatni tekst	Sadrži opis ako TFREVT= L* ili U*

Srodni zadaci

“Upotreba QIPFILTER dnevnika” na stranici 64
i5/OS automatski kreira dnevnik čim prvi put aktivirate filtriranje IP paketa.

Rješavanje problema VPN-a s QVPN dnevnikom

Sadrži informacije o IP prometu i vezama.

VPN koristi poseban dnevnik za zapis informacija o IP prometu i vezama, nazvan QVPN dnevnik. QVPN je pohranjen u QUSRSYS knjižnici. Kod dnevnika je M i tip dnevnika je TS. Rijetko ćete unose ovog dnevnika koristiti svakodnevno. Umjesto toga, možete ustanoviti da su korisni za rješavanje problema i provjeru da vaš sistem, ključevi i

veze funkcioniraju na način koji ste specificirali. Na primjer, unosi dnevnika vam pomažu da shvatite što se događa vašim paketima podataka. Oni vas također informiraju o vašem trenutnom VPN statusu.

Omogućavanje QVPN dnevnika

Sučelje virtualne privatne mreže koristite u System i Navigator za aktivaciju VPN dnevnika.

Ne postoji funkcija koja dozvoljava zapisivanje za sve VPN veze. Zbog toga, morate omogućiti funkciju zapisivanja za svaku pojedinu grupu dinamičkog ključa ili ručne veze.

Sljedeći koraci opisuju kako omogućiti funkciju zapisivanja za određenu grupu dinamičkog ključa ili ručnu vezu:

1. U System i Navigator, proširite **sistem → Mrežu → IP politike → Virtualno privatno umrežavanje → Sigurne veze**.
2. Za grupe dinamičkog ključa, proširite **Po grupi** i zatim desno kliknite grupu dinamičkog ključa za koju želite omogućiti vođenje dnevnika i izaberite **Svojstva.**
3. Za ručne veze, proširite **Sve veze** i zatim desno kliknite ručnu vezu za koju želite omogućiti vođenje dnevnika.
4. Na stranici **Općenito** izaberite razinu vođenja dnevnika koju zahtijevate. Možete birati između četiri opcije. Opcije su:

   Nijedan
   Ne radi se vođenje dnevnika za ovu grupu veze.

   Svi Vođenje dnevnika se radi za sve aktivnosti veze, kao što su pokretanje ili zaustavljanje veze ili osvježavanja ključa, kao i informacije o IP prometu.

   Aktivnost veze
   Vođenje dnevnika se dešava za takve aktivnosti veze kao što su pokretanje ili zaustavljanje veze.

   IP promet
   Vođenje dnevnika se dešava za sav VPN promet koji je pridružen ovoj vezi. Unos u dnevnik se radi svaki put kada se dozove pravilo filtriranja. Sistem zapisuje informacije o IP prometu u dnevnik QIPFILTER, koji je lociran u knjižnici QUSRSYS.
5. Kliknite **OK**.
6. Pokrenite vezu da aktivirate vođenje dnevnika.

Bilješka: Prije prestanka vođenja dnevnika, uvjerite se da veza nije aktivna. Da promijenite status vođenja dnevnika za grupu veze, uvjerite se da nema aktivnih veza koje su pridružene toj određenoj grupi.

Upotreba QVPN dnevnika

Da u dnevniku pogledate detalje specifične za unos, možete na ekranu prikazati unose ili možete koristiti izlaznu datoteku.

Kopiranjem unosa u dnevnik u izlaznu datoteku lako možete pogledati unose koristeći uslužne programe za upit, kao što su Query/400 ili SQL. Također, možete pisati vaše vlastite HLL programe da obradite unose u izlaznim datotekama. Slijedi primjer naredbe Prikaz Dnevnika (DSPJRN):

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

Koristite sljedeće korake za kopiranje unosa VPN dnevnika u izlaznu datoteku:

.

1. Kreirajte kopiju izlazne datoteke dobavljene od sistema, QSYS/QATOVSOF, u korisničkoj knjižnici. Ovo možete napraviti korištenjem naredbe Kreiranje duplikata objekta (CRTDUPOBJ). Slijedi primjer naredbe CRTDUPOBJ:

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

2. Koristite naredbu Prikaz dnevnika (DSPJRN) da kopirate unose iz dnevnika QUSRSYS/QVPN u izlaznu datoteku kreiranu u prethodnom koraku. Ako pokušate kopirati DSPJRN u izlaznu datoteku koja ne postoji, sistem kreira tu datoteku umjesto vas, ali ova datoteka ne sadrži ispravne opise polja.

Srodni koncepti

"Polja QVPN dnevnika"
Pregledajte sljedeću tablicu koja opisuje polja u QVPN izlaznoj datoteci.

Polja QVPN dnevnika

Pregledajte sljedeću tablicu koja opisuje polja u QVPN izlaznoj datoteci.

Ime polja	Dužina polja	Numerički	Opis	Komentari
TSENTL	5	Y	Dužina unosa	
TSSEQN	10	Y	Redni broj	
TSCODE	1	N	Kod dnevnika	Uvijek M
TSENTT	2	N	Tip unosa	Uvijek TS
TSTIME	26	N	SAA vremenska oznaka	
TSJOB	10	N	Ime posla	
TSUSER	10	N	Korisnik posla	
TSNBR	6	Y	Broj posla	
TSPGM	10	N	Ime programa	
TSRES1	51	N	Nije korišten	
TSUSPF	10	N	Ime profila korisnika	
TSSYNM	8	N	Ime sistema	
TSRES2	20	N	Nije korišten	
TSRESA	50	N	Nije korišten	
TSESDL	4	Y	Dužina određenih podataka	
TSCMPN	10	N	VPN komponenta	
TSCONM	40	N	Ime veze	
TSCOTY	10	N	Tip veze	
TSCOS	10	N	Stanje veze	
TSCOSD	8	N	Datum pokretanja	
TSCOST	6	N	Vrijeme pokretanja	
TSCOED	8	N	Datum završetka	
TSCOET	6	N	Vrijeme završetka	
TSTRPR	10	N	Protokol prijenosa	
TSLCAD	43	N	Lokalna adresa klijenta	
TSLCPR	11	N	Lokalni portovi	
TSRCAD	43	N	Udaljena adresa klijenta	
TSCPR	11	N	Udaljeni portovi	
TSLEP	43	N	Lokalna krajnja točka	
TSREP	43	N	Udaljena krajnja točka	
TSCORF	6	N	Osvježena vremena	
TSRFDA	8	N	Datum sljedećeg osvježavanja	

Ime polja	Dužina polja	Numerički	Opis	Komentari
TSRFTI	6	N	Vrijeme sljedećeg osvježavanja	
TSRFLS	8	N	Vijek života osvježenja	
TSSAPH	1	N	SA Faza	
TSAUTH	10	N	Tip provjere autentičnosti	
TSENCR	10	N	Tip šifriranja	
TSDHGR	2	N	Diffie-Hellman grupa	
TSERRC	8	N	Kod greške	

Srodni zadaci

"Upotreba QVPN dnevnika" na stranici 66
Da u dnevniku pogledate detalje specifične za unos, možete na ekranu prikazati unose ili možete koristiti izlaznu datoteku.

Rješavanje VPN-a s VPN dnevnicima posla

Kada naiđete na probleme s vašim VPN vezama, uvijek je preporučljivo da analizirate dnevnike poslova. Zapravo, nekoliko je dnevnika poslova koji sadrže poruke greške i druge informacije koje se odnose na VPN okolinu.

Važno je da analizirate dnevnike posla na obje strane veze, ako su obje strane System i modeli. Kada ne uspije pokretanje dinamičke veze, od velike je pomoći ako razumijete što se događa na udaljenom sistemu.

VPN poslovi, QTOVMAN i QTOKVPNIKE, u izvođenju su na podsistemu QSYSWRK. Možete vidjeti odnosne dnevnike posla sa System i Navigatorom.

Ovaj odlomak predstavlja najvažnije poslove za VPN okolinu. Sljedeći popis pokazuje imena poslova, uz kratka objašnjenja o upotrebi samoga posla:

QTCPIP
Ovaj posao je osnovni posao koji pokreće sva TCP/IP sučelja. Ako imate temeljne probleme općenito za TCP/IP, analizirajte QTCPIP dnevnik posla.

QTOKVPNIKE
Posao QTOKVPNIKE je posao VPN upravitelja ključa. VPN upravitelj ključa sluša UDP port 500 za izvedbu obrade protokola Internet razmjene ključa (IKE).

QTOVMAN
Ovaj posao je upravitelj veze za VPN povezivanja. Dnevnik posla na koji se odnosi sadrži poruke za svaki neuspješni pokušaj povezivanja.

QTPPANSxxx
Ovaj posao se koristi za PPP telefonske veze. On odgovara na pokušaje povezivanja gdje je *ANS definiran u PPP profilu.

QTPPPCTL
Ovo je PPP posao za dial-out veze.

QTPPPL2TP
Ovo je posao upravljanja Sloj 2 Tunelskim protokolom (L2TP). Ako imate problema s postavkom L2TP tunela, potražite poruke u ovom dnevniku posla.

Srodni zadaci

"Kako započeti s VPN rješavanjem problema" na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Uobičajene poruke o greški VPN Upravitelja veze

VPN Upravitelj veze zapisuje dvije poruke u QTOVMAN dnevnik posla kada dođe do greške s VPN povezivanjem.

Prva poruka daje detalje koji se odnose na grešku. Možete pregledati informacije o tim greškama u System i Navigatoru, desnim klikom na vezu s greškom i izborom **Informacije o grešci**.

Druga poruka opisuje akcije koje ste pokušali izvesti na vezi u trenutku kada je došlo do greške. Na primjer, pokretanje ili zaustavljanje veze. Poruke TCP8601, TCP8602 i TCP860A, dole opisane, tipični su primjeri za ove druge poruke.

Poruke o grešci Upravitelja VPN veze

Poruka	Uzrok	Obnavljanje
TCP8601 Ne može pokrenuti VPN vezu [*ime veze*]	Ne mogu pokrenuti ovu VPN vezu zbog jedne od sljedećih šifri razloga: *0* - Prethodna poruka u dnevniku posla s istim imenom VPN veze koja ima detaljnije informacije. *1* - Konfiguracija VPN politike. *2* - Neuspjeh komunikacijske mreže. *3* - VPN Upravitelj ključa nije uspio dogovoriti novu sigurnosnu asocijaciju. *4* - Udaljena krajnja točka za ovu vezu nije ispravno konfigurirana. *5* - VPN Upravitelj ključa se nije uspio odazvati VPN Upravitelju veze. *6* - Neuspjeh učitavanja VPN veze za IP sigurnosnu komponentu. *7* - Neuspjeh PPP komponente.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Ispravite greške i pokušajte zahtjev ponovno. 3. Za pregled statusa veze koristite System i Navigator. Veze koje nisu mogle biti pokrenute bit će u statusu greške.
TCP8602 Greška pri zaustavljanju VPN veze [*ime veze*]	Nakon zahtjeva za zaustavljanjem navedene VPN veze, veza se nije zaustavila ili se zaustavila uz grešku zbog šifre razloga: *0* - Prethodna poruka u dnevniku posla s istim imenom VPN veze koja ima detaljnije informacije. *1* - VPN veza ne postoji. *2* - Neuspjeh interne komunikacije s VPN Upraviteljem ključa. *3* - Neuspjeh interne komunikacije s IPSec komponentom. *4* - Neuspjeh komunikacije s udaljenom krajnjom točkom VPN veze.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Ispravite greške i pokušajte zahtjev ponovno. 3. Za pregled statusa veze koristite System i Navigator. Veze koje nisu mogle biti pokrenute bit će u statusu greške.
TCP8604 Pokretanje VPN veze [*ime veze*] nije uspjelo	Pokretanje VPN veze nije uspjelo zbog jedne od sljedeće šifre razloga: *1* - Ne mogu prevesti ime udaljenog hosta na IP adresu. *2* - Nemogućnost prevođenja imena lokalnog hosta u IP adresu. *3* - Nije učitano pravilo filtriranja VPN politike pridruženo ovoj VPN vezi. *4* - Korisnički definirana vrijednost ključa nije važeća za njegov pridruženi algoritam. *5* - Vrijednost za započinjanje VPN veze ne dozvoljava navedenu akciju. *6* - Uloga sistema kod VPN veze nije konzistentna s informacijom iz grupe veze. *7* - Rezervirano. *8* - Krajnje točke podataka (lokalne i udaljene adrese i usluge) ove VPN veze nisu konzistentne s informacijama od ove grupe veza. *9* - Tip identifikatora nije važeći.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Ispravite greške i pokušajte zahtjev ponovno. 3. Za provjeru ili ispravak konfiguracije VPN politika, koristite System i Navigator. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti.

Poruke o grešci Upravitelja VPN veze

Poruka	Uzrok	Obnavljanje
TCP8605 Upravitelj VPN veze ne može komunicirati s Upraviteljem VPN ključa	VPN Upravitelj veze zahtijeva usluge od VPN Upravitelja ključa za uspostavu sigurnosnih asocijacija za dinamičke VPN veze. VPN Upravitelj veze nije u mogućnosti komunicirati s VPN Upraviteljem ključa.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Provjerite da je *LOOPBACK sučelje aktivno korištenjem naredbe NETSTAT OPTION(*IFC). 3. Zaustavite VPN poslužitelj korištenjem naredbe ENDTCPSVR SERVER(*VPN). Zatim ponovno pokrenite VPN poslužitelj korištenjem naredbe STRTCPSRV SERVER(*VPN). **Bilješka:** Ovo uzrokuje kraj svih VPN veza.
TCP8606 VPN Upravitelj ključa ne može uspostaviti zahtijevanu sigurnosnu asocijaciju veze, [*ime veze*]	VPN Upravitelj ključa ne može uspostaviti zahtijevanu sigurnosnu asocijaciju zbog jednog od ove šifre razloga: *24* - Neuspjela provjera autentičnosti veze ključa VPN Upravitelja ključa. *8300* - Došlo je do greške za vrijeme pregovora oko veze ključem VPN Upravitelja ključa. *8306* - Nije pronađen lokalni unaprijed podijeljeni ključ. *8307* - Nije pronađena udaljena IKE politika faze 1. *8308* - Nije pronađen udaljeni unaprijed podijeljeni ključ. *8327* - Timeout pregovora za ključnu vezu VPN Upravitelja ključa. *8400* - Došlo je do greške za vrijeme pregovora oko VPN veze VPN upravitelja ključa. *8407* - Nije pronađena udaljena IKE politika faze 2. *8408* - Timeout pregovora za VPN vezu VPN Upravitelja ključa. *8500 ili 8509* - Došlo je do greške na mreži VPN Upravitelja ključa.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Ispravite greške i pokušajte zahtjev ponovno. 3. Za provjeru ili ispravak konfiguracije VPN politika, koristite System i Navigator. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti.
TCP8608 VPN veza, [*ime veze*], ne mogu dobiti NAT adresu	Ova grupa dinamičkog ključa ili veza podataka navodi da se prijevod mrežne adrese (NAT) može obaviti na jednoj ili više adresa i da nije uspjela zbog jedne od ovih šifri razloga: *1* - Adresa za primjenu NAT-a nije jednostruka IP adresa. *2* - Sve dostupne adrese su već korištene.	1. Provjerite dnevnike poslova za dodatne poruke. 2. Ispravite greške i pokušajte zahtjev ponovno. 3. Za provjeru ili ispravak VPN politika, koristite System i Navigator. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti za adrese.
TCP8620 Nije dostupna krajnja točka lokalne veze	Nije moguće omogućiti ove VPN veze jer lokalna krajnja točka veze nije dostupna.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Osigurajte da je lokalna krajnja točka veze definirana i pokrenuta korištenjem naredbe NETSTAT OPTION(*IFC). 3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Poruke o grešci Upravitelja VPN veze

Poruka	Uzrok	Obnavljanje
TCP8621 Dostupna krajnja točka lokalnih podataka	Nije moguće omogućiti ove VPN veze jer lokalna krajnja točka za podatke nije dostupna.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Osigurajte da je lokalna krajnja točka veze definirana i pokrenuta korištenjem naredbe NETSTAT OPTION(*IFC). 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8622 Nije dozvoljeno sažimanje pri prijenosu unutar gateway-a	Nije moguće omogućiti ove VPN veze, jer je navedena politika navela način sažimanja prijenosa, a ova je veza definirana kao sigurnosni prilaz.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za promjenu VPN politike, pridružene ovoj VPN vezi, koristite System i Navigator. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8623 VPN veza preklapa se s postojećom	Nije moguće omogućiti ovu VPN vezu jer je postojeća VPN veza već omogućena. Ova veza ima lokalnu krajnju točku podataka [*vrijednost lokalne krajnje točke podataka*] i udaljenu krajnju točku podataka [*vrijednost udaljene krajnje točke podataka*].	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Upotrijebite System i Navigator za pregled svih omogućenih veza koje imaju krajnje točke lokalnih podataka i krajnje točke udaljenih podataka koji preklapaju veze. Ako su zahtijevane obje veze, promijenite politiku postojeće veze. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8624 VPN veza nije u opsegu pridruženog pravila filtera politike	Nije moguće omogućiti VPN vezu jer krajnje točke podataka nisu unutar definiranog pravila filtriranja politike.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za prikaz ograničenja podataka krajnjih točaka ove veze ili grupe dinamičkog ključa koristite System i Navigator. Ako je izabran **Podskup filtera politike** ili **Prilagodi da se podudara filteru politike**, tada provjerite krajnje točke podataka veze. One moraju pristajati unutar aktivnog pravila filtriranja koje ima IPSEC akciju i ime VPN veze pridruženo ovoj vezi. Promijenite politiku postojeće veze ili pravilo filtriranja da omogućite ovu vezu. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Poruke o grešci Upravitelja VPN veze

Poruka	Uzrok	Obnavljanje
TCP8625 VPN veza nije uspjela ESP provjeru algoritma	Nije moguće omogućiti ovu VPN vezu jer tajni ključ pridružen vezi nije bio dovoljan.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za prikaz politike pridružene ovoj vezi i unos drugog tajnog ključa koristite System i Navigator. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8626 Kranja točka VPN veze nije ista kao krajnja točka podataka	Ova VPN veza nije bila moguća, jer politika navodi da je host i da krajnja točka VPN veze nije ista kao krajnja točka podataka.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za prikaz ograničenja podataka krajnjih točaka ove veze ili grupe dinamičkog ključa koristite System i Navigator. Ako je izabran **Podskup filtera politike** ili **Prilagodi da se podudara filteru politike**, tada provjerite krajnje točke podataka veze. One moraju pristajati unutar aktivnog pravila filtriranja koje ima IPSEC akciju i ime VPN veze pridruženo ovoj vezi. Promijenite politiku postojeće veze ili pravilo filtriranja da omogućite ovu vezu. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8628 Nije učitano pravilo filtera politike	Pravilo filtera politike za ovu vezu nije aktivno.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za prikaz aktivnih filtera politike koristite System i Navigator. Provjerite pravilo filtriranja politike za ovu vezu. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8629 IP paket ispušten iz VPN veze	Ova VPN veza ima konfiguriran VPN NAT i zahtijevani skup NAT adresa je premašio dostupne NAT adrese.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Za povećanje broja NAT adresa pridruženih VPN vezi, koristite System i Navigator. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP862A PPP veza nije uspjela s pokretanjem	Ova VPN veza je pridružena PPP profilu. Kada je pokrenuta, učinjen je pokušaj za pokretanje PPP profila, ali došlo je do neuspjeha.	1. Provjerite dnevnike poslova za dodatne poruke ove veze. 2. Provjerite dnevnik posla pridružen PPP vezi. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Srodni zadaci

“Gledanje atributa aktivnih veza” na stranici 55
Ispunite ovaj zadatak da provjerite status i ostale atribute vaših aktivnih veza.

Rješavanje problema VPN-a s praćenjem komunikacija

IBM i5/OS osigurava sposobnost praćenja podataka komunikacijske linije, kao što su sučelja Mreže lokalnog područja (LAN) ili Mreže širokog područja (WAN). Prosječan korisnik možda neće shvatiti cijeli sadržaj podataka praćenja. Međutim, možete koristiti unose praćenja da odredite da li se dogodila razmjena podataka između lokalnih i udaljenih sistema.

Pokretanje praćenja komunikacija

Koristite naredbu Pokretanje praćenja komunikacija (STRCMNTRC) da pokrenete praćenje komunikacija na vašem sistemu. Slijedi primjer naredbe STRCMNTRC:

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

Parametri naredbe su objašnjeni na popisu koji slijedi:

CFGOBJ (Konfiguracijski objekt)
Ime objekta konfiguracije koji se prati. Objekt je ili opis linije, opis mrežnog sučelja ili opis mrežnog poslužitelja.

CFGTYPE (Konfiguracijski tip)
Da li se prati linija (*LIN), mrežno sučelje (*NWI) ili mrežni poslužitelj (*NWS).

MAXSTG (Veličina međuspremnika)
Veličina međuspremnika za praćenje. Default vrijednost je postavljena na 128 KB. Raspon ide od 128 KB do 64 MB. Stvarna maksimalna veličina međuspremnika širom sistema definirana je u sklopu Alata sistemskih usluga (SST). Nadalje, možda ćete primiti poruku greške prilikom korištenja velike veličine međuspremnika na STRCMNTRC naredbi koja je definirana u SST. Imajte na umu da zbroj veličina međuspremnika specificiranih na svih pokrenutim praćenjima komunikacija ne smije premašiti maksimalnu veličinu međuspremnika definiranu u SST-u.

DTADIR (Smjer podataka)
Smjer prometa podataka koji se prati. Smjer može biti samo vanjski promet (*SND), samo ulazni promet (*RCV) ili oba smjera (*BOTH).

TRCFULL (Puno praćenje)
Dešava se kada je međuspremnik praćenja pun. Ovaj parametar ima dvije moguće vrijednosti. Default vrijednost je *WRAP, što znači, kada je međuspremnik praćenja pun, praćenje se premata na početak. Najstariji slogovi praćenja se prepisuju s novima, onim redoslijedom kojim se skupljaju.

Druga vrijednost, *STOPTRC, dozvoljava zaustavljanje praćenja kada je međuspremnik praćenja naveden u parametru MAXSTG pun slogova praćenja. Kao opće pravilo, uvijek definirajte veličinu međuspremnika da bude dovoljno velika da pohrani sve slogove praćenja. Ako se praćenje prekine, možete izgubiti važne informacije praćenja. Ako iskusite problem značajnog obustavljanja, definirajte međuspremnik praćenja da bude dovoljno velik da prematanje međuspremnika ne odbaci bilo koje važne informacije.

USRDTA (Broj korisničkih bajtova za praćenje)
Definira broj podataka koji se prate u dijelu za korisničke podatke okvira podataka. Po defaultu, samo je prvih 100 bajta korisničkih podataka uhvaćeno za LAN sučelja. Za sva druga sučelja su uhvaćeni svi korisnički podaci. Provjerite da ste naveli *MAX ako sumnjate u probleme u korisničkim podacima okvira.

TEXT (Opis praćenja)
Dobavlja značajan opis praćenja.

Zaustavljanje praćenja komunikacija

Ako ne navedete drukčije, praćenje se obično zaustavlja čim se desi uvjet zbog kojeg ste pokrenuli praćenje. Koristite naredbu Zaustavi praćenje komunikacija (ENDCMNTRC) da zaustavite praćenje. Sljedeća naredba je primjer ENDCMNTRC naredbe:

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

Naredba ima dva parametra:

CFGOBJ (Konfiguracijski objekt)
Ime objekta konfiguracije za koji se praćenje izvodi. Objekt je ili opis linije, opis mrežnog sučelja ili opis mrežnog poslužitelja.

CFGTYPE (Konfiguracijski tip)
Da li se prati linija (*LIN), mrežno sučelje (*NWI) ili mrežni poslužitelj (*NWS).

Ispis podataka praćenja

Nakon što zaustavite praćenje komunikacija, trebate ispisati podatke praćenja. Koristite naredbu Ispis praćenja komunikacija (PRTCMNTRC) da izvedete ovaj zadatak. S obzirom da su za vrijeme perioda praćenja uhvaćene sve linije prometa, imate višestruke opcije filtriranja za generiranje izlaza. Pokušajte zadržati spool datoteku što je moguće manjom. To analizu čini bržom i djelotvornijom. U slučaju VPN problema, filtrirajte samo IP promet i ako je moguće samo na određenoj IP adresi. Također, imate opciju filtriranja na određenom broju IP porta. Slijedi primjer naredbe PRTCMNTRC:

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

U ovom primjeru praćenje je formatirano za IP promet i sadrži samo podatke za IP adresu, gdje je izvorna ili odredišna adresa 10.50.21.1, a izvorni ili odredišni broj IP porta je 500.

Niže su objašnjeni samo najvažniji parametri naredbe za analiziranje VPN problema:

CFGOBJ (Konfiguracijski objekt)
Ime objekta konfiguracije za koji se praćenje izvodi. Objekt je ili opis linije, opis mrežnog sučelja ili opis mrežnog poslužitelja.

CFGTYPE (Konfiguracijski tip)
Da li se prati linija (*LIN), mrežno sučelje (*NWI) ili mrežni poslužitelj (*NWS).

FMTTCP (Format TCP/IP podataka)
Da li formatirati praćenje za TCP/IP i UDP/IP podatke. Specificirajte *YES za formatiranje praćenja za IP podatke.

TCPIPADR (Format TCP/IP podataka po adresi)
Ovaj se parametar sastoji od dva elementa. Ako navedete IP adrese na oba elementa, ispisan će biti samo IP promet između tih adresa.

SLTPORT (IP broj porta)
Broj IP porta za filtriranje.

FMTBCD (Format emitiranih podataka)
Da li su svi emitirani okviri ispisani. 'Da' je default. Ako ne želite; na primjer, Address Resolution Protocol (ARP) zahtjeve, navedite *NE; inače vas mogu zasuti opće poruke.

Srodni zadaci

"Kako započeti s VPN rješavanjem problema" na stranici 57
Dovršite ovaj zadatak da naučite razne načine za određivanje bilo kakvih VPN problema koje imate na vašem sistemu.

Srodne informacije za VPN

IBM Redbooks izdanja i Web stranice sadrže informacije koje se odnose na zbirku poglavlja Virtualnog privatnog umrežavanja. Možete pogledati ili ispisati bilo koju od PDF datoteka.

IBM Redbooks

- IBM System i Security Vodič za IBM i5/OS verziju 5 izdanje 4
- AS/400 Internet sigurnost: Implementiranje AS/400 Virtualnih privatnih mreža
- AS/400 Scenariji Internet sigurnosti: Praktičan Approach
- OS/400 V5R2 Virtualne privatne mreže: Udaljeni pristup do IBM eServer iSeries poslužitelja s Windows 2000 VPN klijentima

Web stranica

- TCP/IP za i5/OS: Virtualno privatno umrežavanje
- TCP/IP za i5/OS: RFC dokumente

Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili dodatke o kojima se raspravlja u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području. Bilo koje upućivanje na neki IBM proizvod, program ili uslugu, nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i provjeri rad bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili molbe za patente koje su još u toku, a koje pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakvo pravo na te patente. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci u vezi s dvobajtnim (DBCS) informacijama, kontaktirajte IBM odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pismenom obliku na adresu:

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

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Povremeno se rade promjene na ovim informacijama; te promjene će biti uključene u nova izdanja ove publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

IBM može koristiti ili distribuirati bilo koje informacije koje vi dostavite, na bilo koji način koji smatra prikladnim, bez ikakvih obveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

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

Rochester, MN 55901
U.S.A.

Takve informacije se mogu dobiti, uz odgovarajuće uvjete i termine, uključujući u nekim slučajevima i naplatu.

Licencni program opisan u ovom dokumentu i sav licencirani materijal dostupan za njega je IBM osigurao pod uvjetima IBM Korisničkog ugovora, IBM Međunarodnog programa Ugovora o licenci, IBM Ugovora o licenci za strojni kod ili bilo kojeg jednakovrijednog ugovora s nama.

Podaci o performansama sadržani u ovom dokumentu su utvrđeni u kontroliranom okruženju. Zbog toga se rezultati dobiveni u nekom drugom operativnom okruženju mogu značajno razlikovati. Neka mjerenja su možda napravljena na sistemima razvojne razine i zbog toga nema jamstva da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda procijenjena ekstrapoliranjem. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenjivost podataka na njihovo specifično okruženje.

Informacije koje se odnose na ne-IBM proizvode su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih javno dostupnih izvora. IBM nije testirao te proizvode i ne može potvrditi koliko su točne tvrdnje o performansama, kompatibilnosti ili druge tvrdnje koje se odnose na ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave u vezi budućih IBM namjera ili smjernica su podložne promjeni ili povlačenju bez prethodne obavijesti i predstavljaju samo ciljeve i namjere.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnim poslovnim operacijama. Da bi ih se ilustriralo što je bolje moguće, primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena, a svaka sličnost s imenima i adresama stvarnih poslovnih subjekata u potpunosti je slučajna.

AUTORSKO PRAVO LICENCE:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku, koji ilustriraju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku, bez plaćanja IBM-u, za svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa, u skladu sa sučeljem programiranja aplikacija za operativnu platformu za koju su primjeri programa napisani. Ti primjeri nisu bili temeljito testirani u svim uvjetima. IBM, zbog toga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

Svaka kopija ili bilo koji dio tih primjera programa ili iz njih izvedenih radova, mora uključivati sljedeću napomenu o autorskom pravu:

© (ime vašeg poduzeća) (godina). Dijelovi ovog koda su izvedeni iz IBM Corp. primjera programa. © Autorsko pravo IBM Corp. _unesite godinu ili godine_. Sva prava pridržana.

Ako gledate ove informacije na nepostojanoj kopiji, možda se neće pojaviti fotografije i ilustracije u boji.

Informacije o sučelju programiranja

Ovi dokumenti publikacije virtualnog privatnog umrežavanja su namijenjeni sučeljima programiranja koji korisniku omogućuju pisanje programa za dobivanje usluga za IBM i5/OS.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

Approach
AS/400

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

Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci firme Adobe Systems Incorporated u Sjedinjenim Državama i/ili drugim zemljama.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Ostala imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili oznake usluga drugih.

Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

Osobna upotreba: Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijeđene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU ″KAKVE JESU″ I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Tiskano u Hrvatskoj