

IBM

@server

iSeries

Virtualno privatno umrežavanje

Verzija 5 Izdanje 3





@server

iSeries

Virtualno privatno umrežavanje

Verzija 5 Izdanje 3

Opaska

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene”, na stranici 65.

Šesto izdanje (kolovoz, 2005)

Ovo izdanje se odnosi na verziju 5, izdanje 3, modifikaciju 2 od IBM i5/OS (5722-SS1) i na sva sljedeća izdanja i modifikacije dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC) niti ne radi na CISC modelima.

© **Autorsko pravo International Business Machines Corp. 1998, 2005. Sva prava pridržana.**

Sadržaj

Virtualno privatno umrežavanje. 1

Što je novo za V5R3	2
Ispis ovog poglavlja	3
VPN scenariji	3
VPN scenarij: Osnovno povezivanje grane ureda	4
Detalji konfiguracije	6
VPN scenarij: Osnovno povezivanje posla s poslom	8
Detalji konfiguracije	10
VPN scenarij: Zaštita L2TP dobrovoljnog tunela s IPSec-om	13
Detalji konfiguracije	14
VPN scenarij: Upotreba prijevoda mrežne adrese za VPN	19
VPN koncepti	20
Protokoli IP Sigurnosti (IPSec)	21
Zaglavlje za provjeru autentičnosti	22
Sažimanje tereta sigurnosti	23
AH i ESP kombinirano	24
Upravljanje ključevima	24
Sloj 2 Tunelski Protokol (L2TP)	25
Prijevod mrežne adrese za VPN	26
NAT kompatibilni IPSec	27
IP komprimiranje (IPComp)	28
VPN i IP filtriranje	28
Migracija filtera politika na trenutno izdanje	29
VPN veze bez filtera politike	30
Uključeni IKE	30
Plan za VPN	30
Zahtjevi za VPN postav	31
Određivanje tipa VPN-a za kreiranje	31
Popunjavanje radnih tablica za planiranje VPN-a	32
Radna tablica za planiranje za dinamičke veze	32
Radna tablica za planiranje za ručne veze	33
Konfiguriranje VPN-a	35
Konfiguriranje VPN veze pomoću Čarobnjaka za nove veze	37
Konfiguriranje VPN politika sigurnosti	37
Konfiguriranje politike Internet razmjene ključeva (IKE)	37
Konfiguriranje politike podataka	38
Konfiguriranje sigurne VPN veze	38
Konfiguriranje ručne veze	39
Konfiguriranje VPN paketnih pravila	39
Konfiguriranje pred-IPSec pravila filtriranja	40
Konfiguriranje pravila filtriranja politike	41
Definiranje sučelja za VPN pravila filtriranja	42
Aktiviranje VPN paketnih pravila	42
Pokretanje VPN veze	43
Upravljanje s VPN-om	43

Postavljanje default atributa za vaše veze	43
Resetiranje veze u stanju greške	44
Pogled na informacije o greškama	44
Pogled na atribute aktivnih veza	44
Upotreba praćenja VPN poslužitelja	44
Pogled na dnevnike poslova VPN poslužitelja	45
Pogled na atribute Sigurnosnih udruženja (SA)	45
Zaustavljanje VPN veze	45
Brisanje objekata VPN konfiguracije	45
Rješavanje problema VPN-a	45
Kako započeti rješavanje problema VPN-a	46
Najčešće VPN konfiguracijske greške i kako ih popraviti	47
VPN poruka greške: TCP5B28	48
VPN poruka greške: Stavka nije pronađena	48
VPN poruka greške: PARAMETER PINBUF IS NOT VALID	49
Poruka VPN greške: Stavka nije pronađena, Udaljeni poslužitelj ključa...	49
VPN poruka greške: Ne može se ažurirati objekt	50
VPN poruka greške: Ne može se šifrirati ključ...	50
VPN poruka greške: CPF9821	50
VPN greška: Svi ključevi su praznine	51
VPN greška: javlja se prijava za drugi sistem kod korištenja Paketnih pravila	51
VPN greška: Prazna vrijednost statusa u prozoru iSeries Navigatora	51
VPN greška: Veza ima status omogućeno nakon što ste ju zaustavili.	51
VPN greška: 3DES nije izbor za šifriranje.	51
VPN greška: Neočekivani prikaz stupaca u prozoru iSeries Navigatora	51
VPN greška: Neuspjeh deaktiviranja aktivnih pravila filtriranja	52
VPN greška: Promijenila se grupa veze ključa za ovu vezu	52
Rješavanje problema VPN-a sa QIPFILTER dnevnikom	52
Polja QIPFILTER dnevnika	53
Rješavanje problema VPN-a s QVPN dnevnikom	54
Polja QVPN dnevnika	55
Rješavanje problema VPN-a s dnevnicima poslova	56
Uobičajene poruke o greški VPN Upravitelja veze	57
Rješavanje problema VPN-a praćenjem OS/400 komunikacija	61
Srodne informacije za VPN	63

Dodatak. Napomene 65

Zaštitni znaci	66
Termini i uvjeti za spuštanje i ispis publikacija	67

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. Sa VPN-om vaše poduzeće može kontrolirati mrežni promet i ujedno ponuditi važna svojstva sigurnosti, kao što su provjera autentičnosti i privatnost podataka.

OS/400^(R) VPN je opcijaska komponenta za instalaciju u iSeries^(TM) Navigatoru, grafičkom korisničkom sučelju (GUI) za OS/400. Ona vam dozvoljava da kreirate sigurnu stazu od kraja do kraja između bilo koje kombinacije hosta i prilaza. OS/400 VPN koristi metode provjere autentičnosti, algoritme za šifriranje i druge mjere opreza, da osigura da podaci poslani između dvije krajnje točke njegove veze 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 štite 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 V5R3

Ovo poglavlje opisuje koje su informacije u ovom izdanju nove, ili značajno izmjenjene.

Ispis ovog poglavlja

Ako dajete prednost trajnoj verziji ovih informacija, dođite ovdje za ispis ovog PDF dokumenta.

VPN scenariji

Pregledajte ove scenarije da se upoznate s osnovnim VPN tipovima i koracima uključenim u njihovu konfiguraciju.

VPN koncepti

Važno je da imate barem osnovno znanje standardnih VPN tehnologija. Ovo poglavlje vam daje konceptualne informacije o protokolima koje VPN koristi u svojoj primjeni.

Plan za VPN

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

Konfiguriranje VPN-a

Nakon planiranja za vaš VPN, možete započeti sa njegovim konfiguriranjem. Ovo poglavlje vam daje pregled onoga što možete napraviti s VPN-om i kako to napraviti.

Upravljanje s VPN-om

Ovo poglavlje opisuje različite zadatke koje možete izvoditi da upravljate vašim aktivnim VPN vezama, uključujući opis kako ih promijeniti, nadgledati, ili obrisati.

Rješavanje problema VPN-a

Uputite se na ovo poglavlje kada iskusite probleme s vašim VPN vezama.

Srodne informacije za VPN

Otiđite ovdje za veze na druge izvore VPN informacija i teme koje se na njega odnose.

Što je novo za V5R3

Funkcijska poboljšanja

Poboljšanja za funkciju Verzije 5 Izdanja 3 (V5R3) virtualnih privatnih mreža (VPN) uključuju dva nova tipa identifikatora. Postoje dva nova tipa identifikatora koja se mogu izabrati pri definiciji VPN politike razmjene ključa i krajnjih točaka veze. Tipovi identifikatora uključuju IP adresu i IPv4 ime hosta. Za dodatne informacije pogledajte online pomoć u iSeriesTM Navigatoru.

- **Moja lokalna IP adresa**

Tip identifikatora, Moja lokalna IP adresa, se može izabrati za definiciju tipa lokalnog poslužitelja ključa za politiku Internet razmjene ključeva ili lokalnu krajnju točku podataka u definiciji veze. Kada je izabran, VPN koristi dostupne IPv4 adrese. VPN veze koje koriste ovaj tip identifikatora ne smiju koristiti filter politike. Dodatno, lokalni sistem mora biti začetnik veze.

- **IPv4 ime hosta**

Identifikator IPv4 ime hosta se može izabrati da definira nekoliko drugih parametara:

- Tip identifikatora poslužitelja udaljenog ključa u Politici Internet razmjene ključeva
- Identifikator udaljene adrese u svojstvima veze
- Definicija filtera politike za svojstva grupe veze

IPv4 ime hosta se rješava u IP adresu imena hosta navedenog kao tip identifikatora.

Napomena o VPN sigurnosti:

Preporučljivo je da koristite glavni način pregovaranja kad god se dijeljeni ključ koristi za provjeru autentičnosti. On pruža 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. Za upute kako prisiliti korištenje glavnog načina pregovora pri razmjeni ključeva pogledajte Izlaganje sigurnosti s provjerom autentičnosti preko dijeljenog ključa. Kada kreirate ili mijenjate politiku Internet razmjene ključa, također možete koristiti iSeries Navigator online sistem pomoći za detaljnije informacije .

Informacijska poboljšanja

Promjene poglavlja V5R3 VPN Informacijskog Centra uključuju vizualnu prezentaciju koja objašnjava koncept dobrovoljnog tunela Layer 2 Tunelskog Protokola (L2TP). Koristite se slijedećom vezom za pregled vizualne prezentacije o L2TP dobrovoljnim tunelima zaštićenim s IPSec. Ovo zahtijeva da imate Flash plug-in



. Alternativno možete koristiti HTML verziju ove prezentacije.

Kako vidjeti što je novo ili se promijenilo

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

•



sliku za označavanje početka nove ili promijenjene informacije.

•



sliku za označavanje kraja nove ili promijenjene informacije.

Da pronađete ostale informacije o tome što je novo ili promijenjeno u ovom izdanju, pogledajte Memorandum za korisnike.

Ispis ovog poglavlja

Za pregled ili spuštanje PDF verzije ovog dokumenta, izaberite Virtualno privatno umrežavanje (VPN) (oko 509 KB).

Spremanje PDF datoteka

Da spremite PDF na vašu radnu stanicu za kasnije gledanje i ispis:

1. Desno kliknite PDF u vašem pretražitelju (desno kliknite na vezu iznad).
2. Kliknite **Spremi Cilj kao...** ako koristite Internet Explorer. Kliknite **Spremi Vezu kao...** ako koristite Netscape Communicator.
3. Otiđite do direktorija u koji želite spremiti PDF.
4. Kliknite **Spremi**.

Učitavanje Adobe Acrobat Reader-a

Potreban vam je Adobe Acrobat Reader za pregled ili ispis ovih PDF-ova. Možete spustiti kopiju sa Adobe Web stranice (www.adobe.com/products/acrobat/readstep.html)



VPN scenariji

Pregledajte sljedeće scenarije da se upoznate sa tehničkim i konfiguracijskim detaljima uključenim u svaki od ovih osnovnih tipova veza:

- **VPN scenarij: Osnovno povezivanje grane ureda**
U ovom scenariju vaše poduzeće želi uspostaviti VPN između pod mreža dva udaljena odjela preko para iSeries^(TM) računala koji rade kao VPN prilazi.
- **VPN 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.
- **VPN scenarij: Zaštita L2TP dobrovoljnog tunela s IPSec-om**
Ovaj scenarij ilustrira vezu između hosta grane ureda i korporativnog ureda koji koristi L2TP zaštićen pomoću IPSec-a. Grana ureda ima dinamički dodijeljenu IP adresu, dok korporativni ured ima statičku, globalno usmjerljivu IP adresu.
- **VPN scenarij: Koristite prijevod mrežne adrese za VPN**
U ovom scenariju vaše poduzeće želi izmjenjivati osjetljive podatke s jednim od poslovnih partnera koristeći OS/400^(R) VPN. Da dodatno zaštitite privatnost mrežne strukture vašeg poduzeća, vaše poduzeće će također koristiti VPN NAT da sakrije privatnu IP adresu iSeries poslužitelja kojeg koristi kao host za aplikacije na koje vaš poslovni partner ima pristup.

Još VPN scenarija

Za više scenarija VPN konfiguracija, pogledajte ove ostale izvore informacija za VPN:

- **QoS scenarij: Sigurni i predvidivi rezultati (VPN i QoS)**
Možete kreirati politike kvalitete usluga (QoS) sa vašim VPN-om. Ovaj primjer pokazuje primjer korištenja ovo dvoje zajedno.
- **OS/400 V5R1 Virtualne privatne mreže: Udaljeni pristup na IBM^(R) e(log) poslužitelj iSeries Poslužitelj s Windows^(R) 2000 VPN Klijentima, REDP0153**



Ovaj IBM Redpaper pruža proces konfiguriranja VPN tunela korak po korak koristeći V5R1 VPN i Windows 2000 integriranu L2TP i IPSec podršku.

- **AS/400^(R) Internet sigurnost: Implementiranje AS/400 Virtualnih privatnih mreža, SG24-5404-00**



Ovaj redbook istražuje VPN koncepte i opisuje njihovu primjenu korištenjem IP sigurnosti (IPSec) i Sloj 2 Tunelskog protokola (L2TP) na OS/400.

- **Scenariji Internet Sigurnosti za AS/400: Praktični pristup, SG24-5954-00**



Ovaj redbook istražuje sve integrirane sigurnosne mogućnosti dostupne na OS/400 sistemu kao što su IP filteri, NAT, VPN, HTTP proxy poslužitelj, SSL, DNS, primopredaja pošte, revidiranje i zapisivanje. On opisuje njihovu upotrebu kroz praktične primjere.

VPN scenarij: Osnovno povezivanje grane ureda

Pretpostavite da vaše poduzeće želi smanjiti troškove kojima se izvrgava zbog komunikacije sa i među svojim granama. 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 njegova grana ureda oboje trebaju VPN zaštitu preko Interneta, ali ne i unutar njihovih pojedinih 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 rječima, oni su *granični* ili *rubni* sistemi koji nisu zaštićeni vatrenim zidom. 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 i koja može biti kompanijska privatna mreža ili javni Internet.

Važna opaska:

Ovaj scenarij pokazuje iSeries^(TM) sigurnosne prilaze direktno pripojene na Internet. Namjera neprisutnosti vatrene zida je pojednostavljenje scenarija. To ne podrazumijeva da upotreba vatrene zida nije potrebna. U stvari, uzmite u obzir sigurnosne mjere svaki put kad se spojite na Internet. Pregledajte redbook AS/400^(R) Internet sigurnosni scenariji: Praktičan pristup, SG24-5954-00



, za detaljnije informacije o različitim metodama smanjivanja ovih rizika.

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.
- Korištenje VPN-a omogućava korisnicima pristup na sve poslužitelje i resurse sa bilo koje strane veze, isto kao da su povezani korištenjem iznajmljene linije ili veze mreže širokog područja (WAN).
- Korištenje industrijskog standardnog šifriranja i metoda provjere autentičnosti osigurava sigurnost osjetljivih informacija koje su protekle od jedne lokacije prema drugoj.
- 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 dodjeljivanje vrijednih javnih IP adresa svakom klijentu.

Ciljevi

U ovom scenariju, MyCo, Inc. želi uspostaviti VPN između podmreža svoja dva odjela, Ljudski resursi i Financije,

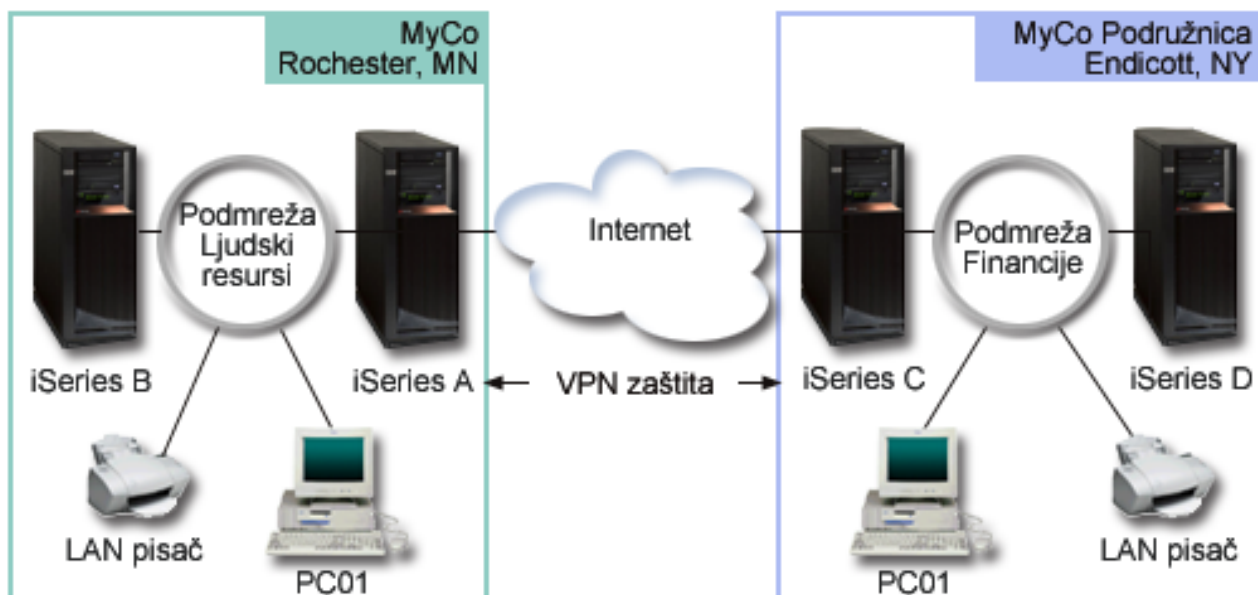
preko para iSeries poslužitelja. Oba će se poslužitelja ponašati kao VPN prilazi. U uvjetima VPN konfiguracija, prilaz obavlja ključno upravljanje i primjenjuje IPSec na podatke koji protječu kroz tunel. Prilazi nisu krajnje točke veze za podatke.

Ciljevi ovog scenarija su sljedeći:

- VPN mora štiti sav promet podataka između pod mreže odjela za Ljudske resurse i pod mreže odjela za Financije.
- Promet podataka ne zahtijeva VPN zaštitu jednom kad dosegne bilo koju od pod mreža ovih odjela.
- Svi klijenti i hostovi na svakoj mreži imaju potpuni pristup na mrežu onog drugog, uključujući sve aplikacije.
- Prilaz poslužitelji mogu međusobno komunicirati i pristupati svojim aplikacijama.

Detalji

Sljedeća slika ilustrira karakteristike mreže od MyCo.



Odjel za ljudske resurse

- iSeries-A se izvodi na OS/400^(R) Verzija 5 Izdanje 2 (V5R2) i ponaša se kao VPN prilaz Odjela za financije.
- Pod mreža je 10.6.0.0 sa maskom 255.255.0.0. Ova pod mreža za podatke predstavlja krajnju točku VPN tunela na MyCo Rochester stranici.
- iSeries-A se povezuje na Internet s IP adresom 204.146.18.227. Ovo je krajnja točka veze. To znači da iSeries-A izvodi ključno upravljanje i primjenjuje IPSec na dolazne i odlazne IP datagrame.
- iSeries-A se povezuje na svoju pod mrežu s IP adresom 10.6.11.1.
- iSeries-B je poslužitelj proizvodnje u mreži Ljudskih resursa koji izvodi standardne TCP/IP aplikacije.

Odjel za financije

- iSeries-C se izvodi na OS/400 Verzija 5 Izdanje 2 (V5R2) i ponaša se kao VPN prilaz Odjela za financije.
- Pod mreža je 10.196.8.0 sa maskom 255.255.255.0. Ova pod mreža za podatke predstavlja krajnju točku VPN tunela na MyCo Endicott stranici.
- iSeries-C se povezuje na Internet s IP adresom 208.222.150.250. Ovo je krajnja točka veze. To znači da iSeries-C izvodi ključno upravljanje i primjenjuje IPSec na dolazne i odlazne IP datagrame.
- iSeries-C se povezuje na svoju pod mrežu s IP adresom 10.196.8.5.

Zadaci konfiguracije

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

1. Provjerite TCP/IP usmjeravanje da osigurate da dva prilaz poslužitelja mogu međusobno komunicirati preko Interneta. Ovo osigurava da se hostovi na svakoj pod mreži ispravno usmjeravaju na njihov odnosni prilaz za pristup udaljenoj pod mreži.
Opaska: Usmjeravanje ne spada u opseg ovog poglavlja. Ako imate pitanja, pogledajte TCP/IP usmjeravanje i uravnoteženje radnog opterećenja u Informacijskom Centru.
2. Popuni radne tablice za planiranje i kontrolne liste za oba sistema.
3. Konfiguriraj VPN na VPN prilazu Ljudskih resursa (iSeries-A).
4. Konfiguriraj VPN na VPN prilazu Financija (iSeries-C).
5. Osigurajte da su VPN poslužitelji pokrenuti.
6. Testiraj komunikacije između dvije udaljene pod mreže.

Detalji konfiguracije

Nakon što dovršite prvi korak, provjeru da TCP/IP usmjeravanje radi ispravno i da vaši gateway poslužitelji mogu komunicirati, spremni ste započeti konfiguriranje VPN-a.

Korak 2: Popunite radne tablice za planiranje

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 sa postavljanjem VPN-a.

Opaska: Ove radne tablice se odnose na iSeries-A, ponovite obradu za iSeries-C i obrnite IP adrese kao što je potrebno.

Kontrolna lista preduvjeta	Odgovori
Da li je vaš OS/400 ^(R) V5R2 (5722-SS1) ili kasniji?	Da
Da li je instalirana opcija Upravitelj digitalnih certifikata (5722-SS1 Opcija 34)?	Da
Da li je instaliran Dobavljač kriptografičkog pristupa (5722-AC2 ili AC3)?	Da
Da li je instaliran iSeries ^(TM) Access for Windows ^(R) (5722-XE1)?	Da
Da li je instaliran iSeries Navigator?	Da
Da li je instalirana podkomponenta Mreža od iSeries Navigatora?	Da
Da li je instaliran Pomoćni program za TCP/IP povezanost za OS/400 (5722-TC1)?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na vašem iSeries (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 vatreni zid ili usmjerivače koji koriste IP filtriranje da li pravila filtriranja vatrene zida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatreni zidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	Da
Da li su vatreni zidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Ove informacije trebate za konfiguraciju VPN-a	Odgovori
Koji tip veze kreirate?	prilaz-prilaz
Kako ćete nazvati grupu dinamičkog ključa?	HRgw2FINgw

Ove informacije trebate za konfiguraciju VPN-a	Odgovori
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 ključeva?	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 ključeva?	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

Korak 3: Konfigurirajte VPN na iSeries-A

Koristite informacije sa vaših radnih tablica za konfiguriranje VPN-a na iSeries-A na sljedeći način:

1. U iSeries Navigatoru proširite iSeries-A —>**Mreža** —>**IP politike**.
2. Desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Nova veza** da započnete Čarobnjaka za novu vezu.
3. Pregledajte stranicu **Dobrodošlice** za informacije o objektima koje čarobnjak kreira.
4. Kliknite **Sljedeće** da odete na stranicu **Ime veze**.
5. U polje **Ime** unesite HRgw2FINgw.
6. (neobvezno) Navedite opis za ovu grupu povezivanja.
7. Kliknite **Sljedeće** da odete na stranicu **scenarij povezivanja**.
8. Izaberite **Povežite vaš prilaz na drugi prilaz**.
9. Kliknite **Sljedeće** da odete na stranicu **Politika Internet razmjene ključeva**.
10. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**.
11. Kliknite **Sljedeće** da odete na stranicu **Certifikat za lokalnu krajnju točku 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** da odete na stranicu **Udaljeni poslužitelj ključeva**.
17. Izaberite **IP adresa Verzija 4** u polju **Tip identifikatora**.
18. Upišite 208.222.150.250 u polju **Identifikator**.
19. Upišite topsecretstuff u polju **Unaprijed podijeljeni 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 **IP verzija 4 podmreža** iz 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 default vrijednosti, zatim kliknite na **Sljedeće** da odete na stranicu **Politika podataka**.
30. Izaberite **Kreiranje nove politike** i zatim izaberite **Uravnoteži sigurnost i izvedbu**. Izaberite **Kreiranje RC4 algoritma za dešifriranje**.
31. Kliknite na **Sljedeće** da odete na stranicu **Primjenljiva sučelja**.
32. Izaberite **TRLINE** iz tablice **Linija**.
33. Kliknite na **Sljedeće** da odete na stranicu **Sažetak**. Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.
34. Kliknite **Završetak** da dovršite konfiguraciju.
35. Kada se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Da, aktiviraj generirane filtere politike**, tada izaberite **Dozvoli sav ostali promet**. Kliknite **OK** da dovršite konfiguraciju. Kada bude zatraženo, navedite da želite aktivirati pravila na svim sučeljima.

Završili ste sa konfiguriranjem VPN-a na iSeries-A. Sljedeći je korak konfiguriranje VPN-a na VPN prilazu Odjela za financije (iSeries-C).

Korak 4: Konfigurirajte VPN na iSeries-C

Sljedite iste korake koje ste koristili za konfiguriranje iSeries-A, uz potrebno obrtanje IP adresa. Za vođenje koristite radne tablice za planiranje. 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 datagrami koje VPN veza mora štititi. Sljedeći je korak pokretanje VPN poslužitelja, ako već nisu pokrenuti.

Korak 6: Pokretanje VPN poslužitelja

Sljedite sljedeće korake da pokrenete VPN poslužitelje:

1. U iSeries Navigatoru proširite **poslužitelj** → **Mreža** → **IP politike**.
2. Desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Pokreni**.

Korak 7: Testiranje veze

Nakon završetka konfiguracije oba poslužitelja te nakon uspješnog pokretanja VPN poslužitelja, provjerite povezanost kako bi osigurali da udaljene podmreže mogu razgovarati jedna s drugom. Da to napravite, sljedite ove korake:

1. U iSeries Navigatoru proširite **iSeries-A** → **Mreža**.
2. Desno kliknite na **TCP/IP Konfiguracija**, izaberite **Uslužni programi** i zatim **Ping**.
3. Iz kućice dijaloga **Ping od**, upišite iSeries-C u polje **Ping**.
4. Kliknite **Ping sada** da provjerite povezanost sa iSeries-A na iSeries-C.
5. Kada završite, kliknite **OK**.

VPN scenarij: Osnovno povezivanje posla s poslom

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 pruža alternativu kompanijama koje 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 sa vašim proizvodnim poduzećem. Ipak, 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. Iskorištavanjem javnog Interneta, možete lako uspostaviti virtualnu privatnu mrežu (VPN), koja će odgovarati 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.

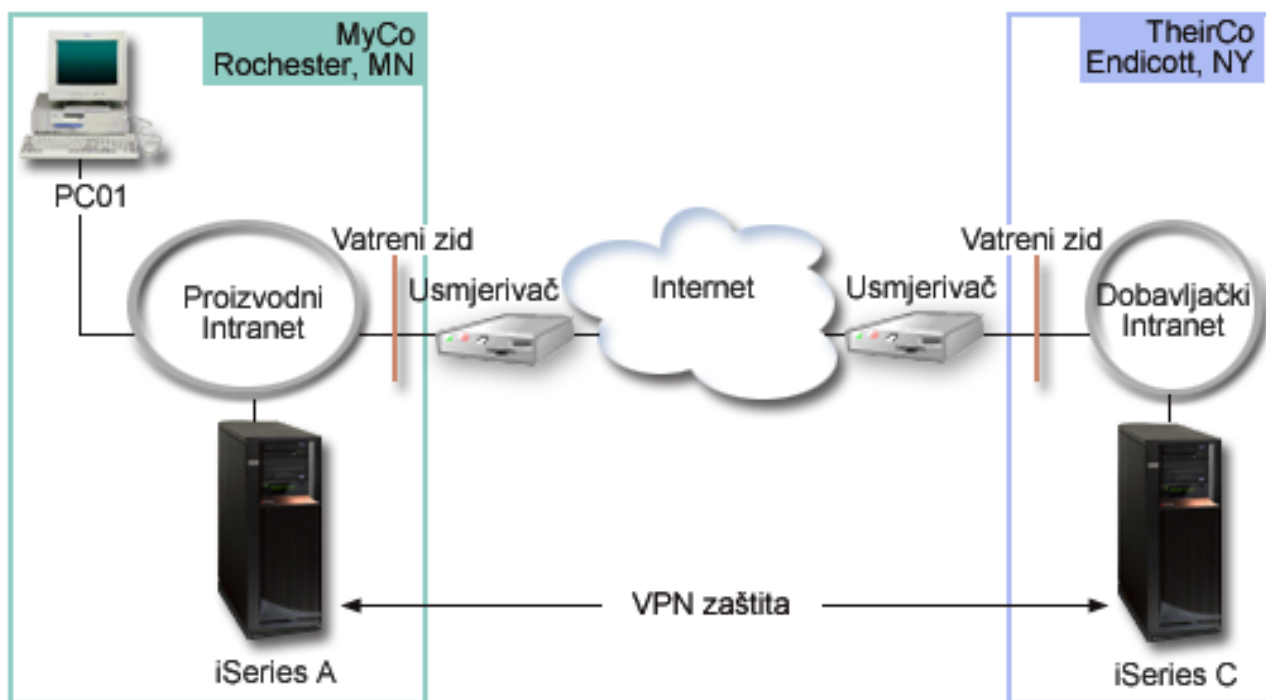
Zbog toga što su informacije koje dijele ova dva poduzeća izuzetno povjerljive, moraju biti zaštićene dok putuju preko Interneta. Dodatno, podaci ne smiju teći nezaštićene kroz mrežu obje kompanije jer svaka strana smatra drugu nepovjerljivom. Drugim riječima, oba poduzeća zahtijevaju provjeru autentičnosti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

Važna opaska:

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

Detalji

Sljedeća slika ilustrira mrežne karakteristike od MyCo i TheirCo:



MyCo Mreža za dobavljanje

- iSeries-A radi na OS/400^(R) Verzija 5 Izdanje 2 (V5R2).
- iSeries-A ima IP adresu 10.6.1.1. Ovo je krajnja točka veze, odnosno krajnja točka za podatke. To znači da iSeries-A izvodi IKE pregovore i primjenjuje IPSec na dolazne i izlazne IP datagrame, a također je izvor i odredište za podatke koji teku kroz VPN.
- iSeries-A je u podmreži 10.6.0.0 sa maskom 255.255.0.0
- Samo iSeries-A može započeti povezivanje sa iSeries-C.

TheirCo Mreža za proizvodnju

- iSeries-C radi na OS/400 Verzija 5 Izdanje 2 (V5R2).
- iSeries-C ima IP adresu 10.196.8.6. Ovo je krajnja točka veze, odnosno krajnja točka za podatke. To znači da iSeries-A izvodi IKE pregovore i primjenjuje IPSec na dolazne i izlazne IP datagrame, a također je izvor i odredište za podatke koji teku kroz VPN.
- iSeries-C je u podmreži 10.196.8.0 sa maskom 255.255.255.0

Zadaci konfiguracije

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

1. Provjerite TCP/IP usmjeravanje da osigurate da iSeries-A i iSeries-C mogu međusobno komunicirati preko Interneta. Ovo osigurava da se hostovi na svakoj podmreži ispravno usmjeravaju na njihov odnosni prilaz za pristup udaljenoj podmreži. Budite na oprezu s ovim scenarijom, trebate uzeti u obzir usmjeravanje privatnih adresa koje prije niste imali.

Opaska: Usmjeravanje ne spada u opseg ovog poglavlja. Ako imate pitanja, pogledajte TCP/IP usmjeravanje i uravnoteženje radnog opterećenja u Informacijskom Centru.

2. Popunite radne tablice za planiranje i kontrolne liste za oba sistema.
3. Konfigurirajte VPN na iSeries-A u MyCo Mreži za dobavljanje.
4. Konfigurirajte VPN na iSeries-C u TheirCo Mreži za proizvodnju.
5. Aktivirajte pravila filtriranja na oba poslužitelja.
6. Pokrenite povezivanje sa iSeries-A.
7. Testirajte komunikacije između dvije udaljene podmreže.

Detalji konfiguracije

Nakon što dovršite prvi korak, verificiranje da TCP/IP usmjeravanje radi ispravno i da vaši poslužitelji mogu komunicirati, spremni ste započeti konfiguriranje VPN-a.

Korak 2: Popunite radne tablice za planiranje

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 sa postavljanjem VPN-a.

Opaska: Ove radne tablice se odnose na iSeries-A, ponovite obradu za iSeries-C i obrnite IP adrese kao što je potrebno.

Kontrolna lista preduvjeta	Odgovori
Da li je vaš OS/400 ^(R) V5R2 (5722-SS1) ili kasniji?	Da
Da li je instalirana opcija Upravitelj digitalnih certifikata (5722-SS1 Opcija 34)?	Da
Da li je instaliran Dobavljač kriptografičkog pristupa (5722-AC2 ili AC3)?	Da
Da li je instaliran iSeries ^(TM) Access for Windows ^(R) (5722-XE1)?	Da
Da li je instaliran iSeries Navigator?	Da
Da li je instalirana podkomponenta Mreža od iSeries Navigatora?	Da
Da li je instaliran Pomoćni program za TCP/IP povezanost za OS/400 (5722-TC1)?	Da
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	Da
Da li je TCP/IP konfiguriran na vašem iSeriesu (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 vatreni zid ili usmjerivače koji koriste IP filtriranje da li pravila filtriranja vatrene zida ili usmjerivača podržavaju AH i ESP protokole?	Da
Da li su vatreni zidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	Da
Da li su vatreni zidovi konfigurirani da omoguće IP prosljeđivanje?	Da

Ove informacije trebate za konfiguraciju VPN-a	Odgovori
Koji tip veze kreirate?	host-host
Kako ćete nazvati grupu dinamičkog ključa?	MyCo2TheirCo
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?	Da
Koji je identifikator za lokalnog poslužitelja ključa?	IP adresa: 10.6.1.1
Koji je identifikator za lokalnu krajnju točku podataka?	IP adresa: 10.6.1.1
Koji je identifikator udaljenog poslužitelja ključa?	IP adresa: 10.196.8.6
Koji je identifikator za udaljenu krajnju točku podataka?	IP adresa: 10.196.8.6
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

Korak 3: Konfigurirajte VPN na iSeries-A

Koristite informacije sa vaših radnih tablica za konfiguriranje VPN-a na iSeries-A na sljedeći način:

1. U iSeries Navigatoru proširite →**Mreža** →**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Nova veza** da započnete Čarobnjaka za vezu.
3. Pregledajte stranicu **Dobrodošlice** za informacije o objektima koje čarobnjak kreira.
4. Kliknite **Sljedeće** da odete na stranicu **Ime veze**.
5. U polje **Ime** upišite MyCo2TheirCo.
6. (neobvezno) Navedite opis za ovu grupu povezivanja.
7. Kliknite **Sljedeće** da odete na stranicu **scenarij povezivanja**.
8. Izaberite **Povežite vaš host na drugi host**.
9. Kliknite **Sljedeće** da odete na stranicu **Politika Internet razmjene ključeva**.
10. Izaberite **Kreiranje nove politike** i zatim izaberite **Najviša sigurnost, najniža izvedba**.
11. Kliknite **Sljedeće** da odete na stranicu **Certifikat za lokalnu krajnju točku veze**.
12. Izaberite **Da** da naznačite da nećete koristiti certifikate za provjeru autentičnosti veze. Zatim izaberite certifikat koji predstavlja iSeries-A.
Opaska: Ako želite koristiti certifikat za provjeru autentičnosti lokalne krajnje točke 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, ova informacija je definirana u certifikatu koji kreirate u DCM-u.
15. Kliknite **Sljedeće** da odete na stranicu **Udaljeni poslužitelj ključeva**.
16. Izaberite **IP adresa Verzija 4** u polju **Tip identifikatora**.
17. Upišite 10.196.8.6 u polju **Identifikator**.
18. Kliknite **Sljedeće** da odete na stranicu **Usluge podataka**.
19. Prihvatite default vrijednosti, zatim kliknite na **Sljedeće** da odete na stranicu **Politika podataka**.
20. Izaberite **Kreiranje nove politike** i zatim izaberite **Najviša sigurnost, najniža izvedba**. Izaberite **Kreiranje RC4 algoritma za dešifriranje**.
21. Kliknite na **Sljedeće** da odete na stranicu **Primjenljiva sučelja**.
22. Izaberite **TRLINE**.
23. Kliknite **Sljedeće** da odete na stranicu **Sažetak**. Pregledajte objekte koje će čarobnjak kreirati da osigurate da su ispravni.

24. Kliknite **Završetak** da dovršite konfiguraciju.
25. Kada se pojavi kućica dijaloga **Aktiviranje filtera politike**, izaberite **Ne, aktiviraj pravila paketa u neko drugo vrijeme**, tada izaberite **OK**.

Sljedeći korak je specificiranje da samo iSeries-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** da spremite vaše promjene.

Završili ste sa konfiguriranjem VPN-a na iSeries-A. Sljedeći je korak konfiguriranje VPN-a na iSeries-C u TheirCo Proizvodnoj mreži.

Korak 4: Konfigurirajte VPN na iSeries-C

Slijedite iste korake koje ste koristili za konfiguriranje iSeries-A, uz potrebno obrtanje IP adresa. Za vođenje koristite radne tablice za planiranje. Kada završite konfiguriranje za iSeries-C, morate aktivirati pravila filtriranja koja je Čarobnjak za veze kreirao na svakom poslužitelju.

Korak 5: Aktivirajte paketna pravila

Čarobnjak automatski kreira paketna pravila koja ova veza zahtijeva za ispravan rad. Ipak, njih morate aktivirati na oba sistema prije nego možete pokrenuti VPN vezu. Da to napravite na iSeries-A, slijedite ove korake:

1. U iSeries Navigatoru proširite **iSeries-A** → **Mreža** → **IP politike**.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje pravila paketa**.
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 iSeries-C.

Korak 6: Pokretanje veze

Slijedite sljedeće korake da pokrenete MyCo2TheirCo vezu sa iSeries-A:

1. U iSeries Navigatoru proširite **iSeries-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*. Vezi bi moglo trebati do nekoliko minuta za pokretanje, zato povremeno radite osvježavanje sve dok se status ne promijeni u *Omogućeno*.

Korak 7: Testiranje veze

Nakon završetka konfiguracije oba poslužitelja te nakon uspješnog pokretanja connection poslužitelja, provjerite povezanost kako bi osigurali da udaljene pod mreže mogu razgovarati jedna s drugom. Da to napravite, slijedite ove korake:

1. U iSeries Navigatoru proširite **iSeries-A** —>**Mreža**.
2. Desno kliknite na **TCP/IP Konfiguracija**, izaberite **Uslužni programi** i zatim **Ping**.
3. Iz kućice dijaloga **Ping od**, upišite iSeries-C u polje **Ping**.
4. Kliknite **Ping sada** da provjerite povezanost sa iSeries-A na iSeries-C.
5. Kada završite, kliknite **OK**.

VPN scenarij: Zaštita L2TP dobrovoljnog tunela s IPSec-om

Pretpostavite da vaše poduzeće ima manju granu ureda u drugoj državi. U toku cijelog radnog dana podružnica može zahtijevati pristup tajnim podacima o iSeries^(TM) unutar vašeg korporativnog Intraneta. Vaše poduzeće trenutno koristi skupe iznajmljene linije da omogući grani ureda 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 može biti učinjeno kreiranjem Sloj 2 Tunelskog protokola (L2TP) dobrovoljnog tunela koji proširuje vašu korporativnu mrežu, tako da se čini da je grana ureda dio vaše korporativne pod mreže. VPN štiti promet podacima preko L2TP tunela.

Pomoću L2TP dobrovoljnog tunela, udaljena grana ureda postavlja tunel direktno na L2TP mrežni poslužitelj (LNS) korporativne mreže. Funkcionalnost L2TP koncentratora pristupa (LAC) prebiva na klijentu. Tunel je transparentan za Dobavljača Internet usluga (ISP) udaljenog klijenta, zato nije potrebno da ISP podržava L2TP. Ako želite čitati više o L2TP konceptima, pogledajte Sloj 2 Tunelski protokol (L2TP).

Važna opaska:

Ovaj scenarij pokazuje iSeries sigurnosne prilaze direktno pripojene na Internet. Namjera neprisutnosti vatrenog zida je pojednostavljenje scenarija. To ne podrazumijeva da upotreba vatrenog zida nije potrebna. Uzmite u obzir sigurnosne mjere svaki put kad se spojite na Internet. Pregledajte redbook AS/400^(R) Internet sigurnosni scenariji: Praktičan pristup, SG24-5954-00



, za detaljnije informacije o različitim metodama smanjivanja ovih rizika.

Ciljevi

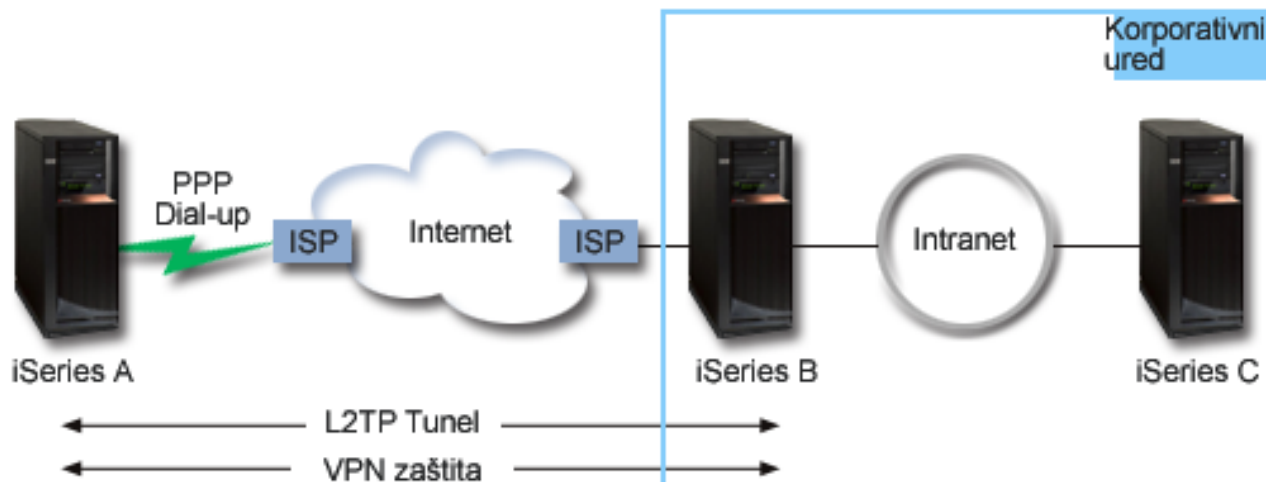
U ovom scenariju iSeries poslužitelj grane ureda spaja se na svoju korporativnu mrežu preko prilaz iSeries poslužitelja sa L2TP tunelom zaštićenim pomoću VPN-a.

Glavni ciljevi ovog scenarija su:

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

Detalji

Sljedeća slika ilustrira mrežne karakteristike za ovaj scenarij:



iSeries-A

- Mora imati pristup TCP/IP aplikacijama na svim sistemima na korporativnoj mreži.
- Prima dinamički dodijeljene IP adrese od svog ISP-a.
- Mora biti konfiguriran da omogući L2TP podršku.

iSeries-B

- Mora imati pristup TCP/IP aplikacijama na iSeries-a poslužitelju.
- Podmreža je 10.6.0.0 sa 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 iSeries-B izvodi upravljanje ključem i primjenjuje IPSec na dolazne i odlazne IP datagrame. iSeries-B se povezuje na svoju podmrežu s IP adresom 10.6.11.1.

U L2TP terminima, *iSeries-A* se ponaša kao L2TP inicijator, dok se *iSeries-B* ponaša kao L2TP završnik.

Zadaci konfiguracije

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

1. Konfiguriraj VPN (stranica 14) na iSeries-A poslužitelju.
2. Konfiguriraj PPP (stranica 16) profil veze i virtualnu liniju za iSeries-A poslužitelj.
3. Primijeni (stranica 17) grupu dinamičkog ključa na PPP profil.
4. Konfiguriraj VPN (stranica 17) na iSeries-B poslužitelju.
5. Konfiguriraj PPP (stranica 18) profil veze i virtualnu liniju za iSeries-B poslužitelj.
6. Aktiviraj (stranica 18) paketna pravila na iSeries-A i iSeries-B poslužiteljima.
7. Pokreni (stranica 19) vezu sa iSeries-A poslužitelja.

Detalji konfiguracije

Nakon što verificirate da TCP/IP radi ispravno i da vaši iSeries^(TM) poslužitelji mogu komunicirati, spremni ste započeti konfiguriranje veze opisane u ovom scenariju.

Korak 1: Konfigurirajte VPN na iSeries-A

Slijedite sljedeće korake da konfigurirate VPN na iSeries-A poslužitelju:

1. **Konfigurirajte politiku Internet razmjene ključa**

- a. U iSeries Navigatoru proširite iSeries-A → Mreža → IP politike → Virtualno privatno umrežavanje → Politike IP Sigurnosti.
- b. Desno kliknite **Politike Internet razmjene ključeva** i izaberite **Nova politika Internet razmjene ključa**.
- c. Na stranici **Udaljeni poslužitelj** izaberite **Verzija 4 IP adresa** kao tip identifikatora i zatim upišite 205.13.237.6 u polju **IP adresa**.
- d. Na stranici **Udruženja** 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, thisisthekeyid. Zapamtite da lokalni poslužitelj ključa ima dinamički dodijeljenu IP adresu koju je nemoguće unaprijed znati. iSeries-B koristi identifikator da identificira iSeries-A kada iSeries-A započinje vezu.
- g. Na stranici **Pretvorbe** kliknite **Dodaj** da dodate pretvorbe koje iSeries-A predlaže iSeries-B poslužitelju za zaštitu ključa i da navede da li IKE politika koristi zaštitu identiteta kod iniciranja pregovora 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)**.



Opaska: Ako morate koristiti dijeljene ključeve i agresivniji način pregovaranja, izaberite takve lozinke koje će se teško otkriti pri napadima koji koriste rječnik za otkrivanje lozinke. Također se preporučuje da periodički mijenjate vaše lozinke.



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

2. Konfiguriranje politike podataka

- a. Sa VPN sučelja desno kliknite **Politike podataka** i izaberite **Nova politika podataka**.
- b. Na stranici **Općenito** navedite ime politike podataka. Na primjer, l2tpremoteuser.
- 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** da dodate pretvorbu politike podataka.
- e. Izaberite **Prijenos** za način sažimanja.
- f. Navedite vrijednost za istek ključa.
- g. Kliknite **OK** da se vratite na stranicu **Pretvorbe**.
- h. Kliknite **OK** da spremite vašu novu politiku podataka.

3. Konfiguriranje grupe dinamičkog ključa

4.

- a. Sa 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 drugom koraku, **l2tpremoteuser**, iz padajuće liste **Politika podataka**.
- g. Izaberite **Lokalni sistem započinje vezu** da označite da samo iSeries-A može započeti veze sa iSeries-B poslužiteljem.
- 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**.

Sada trebate dodati vezu u grupu koji ste upravo kreirali.

5. Konfiguriranje grupe dinamičke veze

- a. Sa VPN sučelja proširite **Po grupi**. Ovo prikazuje popis svih grupa dinamičkog ključa koje ste konfigurirali na iSeries-A poslužitelju.
- 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** iz padajuće liste **Protokol**.
- l. Kliknite **OK** da kreirate vezu dinamičkog ključa.

Završili ste sa konfiguriranjem VPN-a na iSeries-A. Sljedeći je korak konfiguriranje PPP profila za iSeries-A.

Korak 2: Konfigurirajte profil PPP veze i virtualnu liniju na iSeries-A

Ovaj odlomak opisuje korake koje morate poduzeti za kreiranje PPP profila za iSeries-A. PPP nema njemu pridruženu fizičku liniju; umjesto toga, on koristi virtualnu liniju. To je zato što PPP promet tunelira kroz L2TP tunel, dok VPN štiti L2TP tunel.

Sljedite sljedeće korake za kreiranje profila PPP veze za iSeries-A poslužitelj:

1. U iSeries Navigatoru proširite iSeries-A → **Mreža** → **Usluge daljinskog 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 odredite veze. U ovom slučaju, upišite **toCORP**. Ime koje navedete mora imati 10 ili manje znakova.
8. (neobvezno) Navedite opis za profil.
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. Otvoriti će se kućica dijaloga **Svojstva L2TP linije**.
11. Na stranici **Općenito** upišite opis za virtualnu liniju.
12. Otiđite na stranicu **Provjera autentičnosti**.
13. U polju **Ime lokalnog hosta** upišite ime hosta lokalnog poslužitelja ključa, **iSeriesA**.
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 **Zahtjeva IPsec zaštitu** i izaberite grupu dinamičkog ključa kreiranu u prvom koraku, **l2tptocorp** i padajuće liste **Ime grupe za vezu**.
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 pod mreži.
20. U odlomku za usmjeravanje, izaberite **Definiraj dodatne statičke smjerove** i kliknite **Smjerovi**. Ako nisu dane informacije o usmjeravanju u PPP profilu, tada je iSeries-A u mogućnosti doseći samo krajnje točke udaljenog tunela, ali niti jedan drugi sistem na **10.6.0.0** pod mreži.
21. Kliknite **Dodaj** da dodate unos za statički smjer.
22. Upišite pod mrežu, **10.6.0.0** i masku pod mreže **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 **Protokol provjere autentičnosti za upotrebu** izaberite **Zahtjevaj šifriranu lozinku (CHAP-MD5)**
28. Upišite korisničko ime, **iSeriesA** i lozinku.
29. Kliknite **OK** da spremite PPP profil.

Korak 3: Primijenite l2tptocorp grupu dinamičkog ključa na PPP profil toCorp

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 to napravite, slijedite ove korake:

1. Upravljajte do VPN sučelja, zatim proširite **Sigurne veze**—>**Po grupi**.
2. Desno kliknite grupu dinamičkog ključa, **l2tptocorp** i izaberite **Svojstva**.
3. Otiđite na stranicu **Sučelja** i izaberite **Primijeni ovu grupu** za PPP profil koji ste kreirali u drugom koraku, **toCorp**.
4. Kliknite **OK** da primijenite **l2tptocorp** na PPP profil, **toCorp**.

Korak 4: Konfigurirajte VPN na iSeries-B

Slijedite iste korake koje ste koristili za konfiguriranje iSeries-A, uz potrebno obrtanje IP adresa i identifikatora. Uzmite ove ostale točke u obzir prije nego započnete:

- Identificirajte udaljeni poslužitelj ključa po identifikatoru ključa koji ste naveli za poslužitelj lokalnog ključa na iSeries-A poslužitelju. Na primjer, `thisisthekeyid`.
- Koristite *točno* isti unaprijed podijeljeni ključ.
- Uvjerite se da se vaše pretvorbe podudaraju s onima koje ste konfigurirali na iSeries-A, ili veza 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.

Korak 5: Konfigurirajte profil PPP veze i virtualnu liniju na iSeries-B

Slijedite sljedeće korake za kreiranje profila PPP veze za iSeries-B poslužitelj:

1. U iSeries Navigatoru proširite iSeries-B → **Mreža** → **Usluge daljinskog 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 **Završnik (mrežni poslužitelj)** iz padajuće liste **Operacijski način**.
6. Kliknite **OK** na stranicama svojstva PPP profila.
7. Na stranici **Općenito** upišite ime koje identificira tip i odredite veze. U ovom slučaju, upišite `tobran`. Ime koje navedete mora imati 10 ili manje znakova.
8. (neobvezno) Navedite opis za profil.
9. Otiđite na stranicu **Veza**.
10. Izaberite IP adresu krajnje točke lokalnog tunela, `205.13.237.6`.
11. U polju **Ime virtualne linije** izaberite **tobran** 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. Otvoriti će se kućica dijaloga **Svojstva L2TP linije**.
12. Na stranici **Općenito** upišite opis za virtualnu liniju.
13. Otiđite na stranicu **Provjera autentičnosti**.
14. U polju **Ime lokalnog hosta** upišite ime hosta lokalnog poslužitelja ključa, `iSeriesB`.
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 dodjeljene 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 **Protokol provjere autentičnosti za upotrebu** izaberite **Zahtjevaj šifriranu lozinku (CHAP-MD5)**.
23. Upišite korisničko ime, `iSeriesB` i lozinku.
24. Kliknite **OK** da spremite PPP profil.

Korak 6: Aktivirajte paketna pravila

VPN automatski kreira paketna pravila koja ova veza zahtijeva za ispravan rad. Ipak, njih morate aktivirati na oba sistema prije nego možete pokrenuti VPN vezu. Da to napravite na iSeries-A, slijedite ove korake:

1. U iSeries Navigatoru proširite **iSeries-A** → **Mreža** → **IP politike**.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje pravila paketa**.

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 iSeries-B.

Korak 7: Pokretanje veze

Konačni korak je pokretanje veze. Prije nego možete započeti L2TP vezu, morate omogućiti L2TP završniku da odgovori na zahtjeve inicijatora. Nakon što osigurate da su sve potrebne usluge pokrenute, pokrenite PPP vezu na strani završnika. Sljedeći koraci opisuju kako započeti PPP vezu na iSeries-B:

1. U iSeries Navigatoru proširite iSeries-B →**Mreža**→**Usluge daljinskog pristupa**.
2. Kliknite **Profili veze odzivnika** da prikazete popis profila odzivnika u desnom oknu.
3. Desno kliknite **tobran** i izaberite **Pokreni**. Nakon što započne profil veze, prozor se osvježava i pokazuje vezu kao **Čekanje na zahtjeve za vezom**. iSeries-A sada može odgovoriti na L2TP zahtjeve za vezom sa iSeries-B poslužitelja.

Slijedite sljedeće korake da pokrenete L2TP vezu na iSeries-A poslužitelju:

1. U iSeries Navigatoru proširite iSeries-A →**Mreža**→**Usluge daljinskog pristupa**.
2. Kliknite **Profili veze davaoca** da prikazete popis profila davaoca u desnom oknu.
3. Desno kliknite **toCORP** i izaberite **Pokreni**. Nakon što započne profil veze, prozor se osvježava i pokazuje vezu kao **Uspostavljanje L2TP tunela**.
4. Pritisnite F5 za osvježavanje ekrana. Ako je L2TP tunel uspješno pokrenut, status veze sada će glasiti **Aktivne veze**.

VPN scenarij: Upotreba prijevoda mrežne adrese za VPN

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 dodatno zaštitite privatnost mrežne strukture vašeg poduzeća, vi odlučujete da trebate sakriti privatnu IP adresu vaše iSeries^(TM) koja poslužuje aplikacije kojima dobavljač ima pristup. Pitanje je: Kako napraviti da ovo proradi?

Odgovor: OS/400^(R) VPN. Koristite ga ne samo da kreirate definicije veze na VPN prilazu na mreži vašeg poduzeća, već i da omogućite prijevod adresa koji trebate da sakrijete vaše lokalne privatne adrese. Za razliku od konvencionalnog prijevoda mrežne adrese (NAT), koji mijenja IP adrese u sigurnosnim udruženjima (SA) koja VPN zahtjeva za funkcioniranje, VPN NAT obavlja prijevod adresa prije SA provjere valjanosti, dodjelom adrese vezi kada se veza pokrene.

Ciljevi

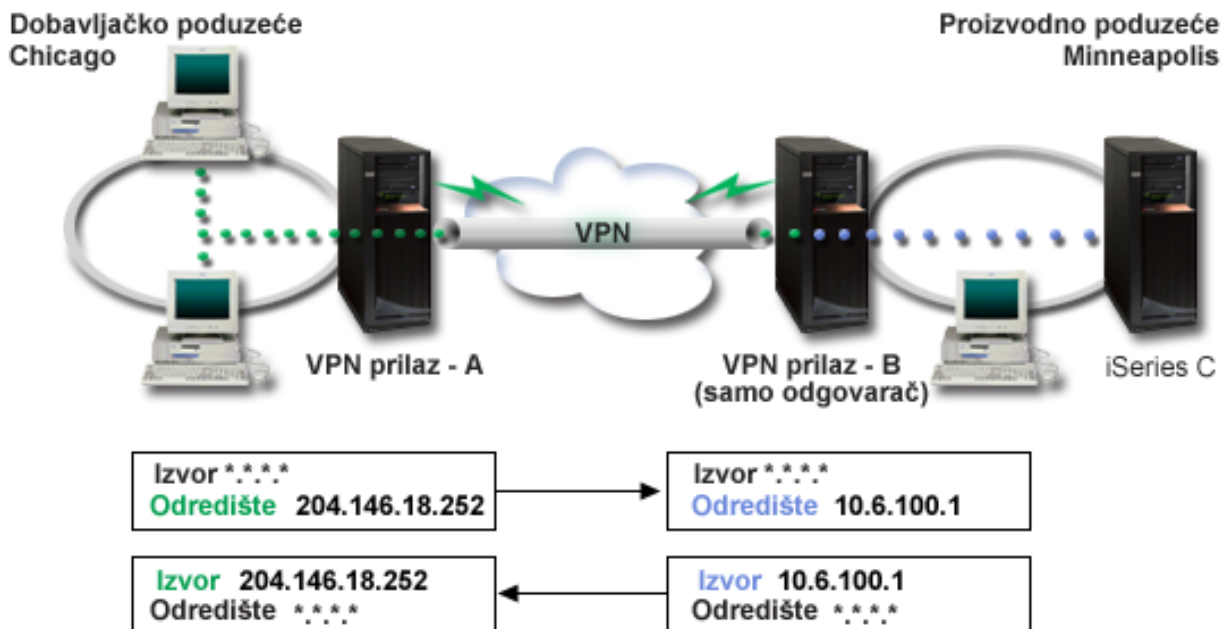
Ciljevi ovog scenarija su da:

- dozvoli svim klijentima u mreži dobavljača pristup jednom host iSeries poslužitelju u mreži proizvođača preko prilaz-prilaz VPN veze.

- sakrije privatnu IP adresu host iSeries poslužitelja u mreži proizvođača, njenim prijevodom u javnu IP adresu korištenjem prijevoda mrežne adrese za VPN (VPN NAT).

Detalji

Sljedeći dijagram ilustrira mrežne karakteristike za oboje, mrežu dobavljača i mrežu proizvođača:



- VPN prilaz-A je konfiguriran da uvijek započne veze na VPN prilaz-B.
- VPN prilaz-A definira odredišnu krajnju točku za vezu kao 204.146.18.252 (javna adresa dodijeljena iSeries-C poslužitelju).
- iSeries-C ima privatnu IP adresu u mreži proizvođača, 10.6.100.1.
- Javna adresa 204.146.18.252 definirana je u spremištu za lokalnu uslugu na VPN prilazu-B za privatnu adresu iSeries-C poslužitelja, 10.6.100.1.
- VPN prilaz-B prevodi javnu adresu iSeries-C poslužitelja u njegovu privatnu adresu, 10.6.100.1, za ulazne datagrame. VPN prilaz-B prevodi povratne, izlazne, datagrame iz 10.6.100.1 natrag na javnu adresu iSeries-C poslužitelja, 204.146.18.252. Što se tiče klijenata u mreži dobavljača, iSeries-C ima IP adresu 204.146.18.252. Oni nikad neće biti svjesni da se desio prijevod adresa.

Zadaci za konfiguraciju

Morate dovršiti svaki od sljedećih zadataka da konfigurirate vezu opisanu u ovom scenariju:

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

VPN koncepti

Virtualno privatno umrežavanje (VPN) koristi nekoliko važnih TCP/IP protokola da zaštiti promet podataka. Da bi bolje razumjeli kako radi svaka VPN veza, upoznajte se sa ovim protokolima i konceptima te kako ih OS/400^(R) VPN koristi:

- **Protokoli IP Sigurnost (IPSec)**
IPSec daje stabilnu, dugotrajnu osnovu za omogućavanje sigurnosti slojeva mreže.

- **Upravljanje ključem**
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.
- **Sloj 2 Tunelski protokol (L2TP)**
Ako planirate koristiti VPN vezu za sigurnu komunikaciju između vaše mreže i udaljenih klijenata, morate biti upoznati i sa L2TP.
- **Prijevod mrežne adrese za VPN (VPN NAT)**
OS/400 VPN omogućuje načine za obavljanje prijevoda mrežne adrese, zvanog 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.
- **UDP sažimanje**
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.
- **IP komprimiranje (IPComp)**
IPComp smanjuje veličinu IP datagrama komprimiranjem datagrama, da se povećaju performanse komunikacije između dva VPN partnera.
- **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 sa VPN-om.

Protokoli IP Sigurnosti (IPSec)

IPSec daje stabilnu, dugotrajnu osnovu za omogućavanje sigurnosti slojeva mreže. Podržava sve kriptografske algoritme koji su danas u upotrebi, a može također smjestiti i novije, moćnije algoritme kada budu postali dostupni. IPSec protokoli adresiraju ova glavna pitanja sigurnosti:

Provjera autentičnosti porijekla podataka

Provjerava da svaki datagram potiče od navedenog odašiljača.

Integritet podataka

Provjerava da sadržaji datagrama nisu promijenjeni u prijenosu, bilo namjerno, ili zbog slučajnih pogrešaka.

Povjerljivost podataka

Skriva sadržaj poruke, najčešće korištenjem šifriranja.

Zaštita od ponovljenog izvođenja

Osigurava da napadač ne može presresti datagram i izvoditi ga u nekom naknadnom trenutku

Automatizirano upravljanje kriptografskim ključevima i sigurnosnim udruženjima

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 udruženja (SA) i automatiziranu generaciju i osvježavanje kriptografskih ključeva.

Glavni IPSec protokoli navedeni su na donjem popisu:

- **Protokol Zaglavlje za provjeru autentičnosti (AH)**
- **Protokol Sažimanje tereta sigurnosti (ESP)**
- **Kombiniranje AH i ESP protokola**
- **Protokoli Internet razmjene ključa (IKE)**

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira IPSec u Zahtjevu za komentarima (RFC) 2401, *Sigurnosna arhitektura za Internet protokol*. Ovaj RFC možete pogledati na Internetu na sljedećoj Web stranici: <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. Ipak, AH ne omogućava povjerljivost podataka, što znači da se svi vaši podaci šalju u razgovjetnom obliku.

AH osigurava integritet podataka pomoću kontrolne sume koju generira kod za provjeru autentičnosti poruke, kao na primjer MD5. Da osigura provjeru autentičnosti porijekla podataka, AH u algoritam uključuje tajni podijeljeni ključ koji koristi za provjeru autentičnosti. Da osigura zaštitu od ponovljenog izvođenja, AH koristi polje za redni broj unutar AH zaglavlja. Ovdje ništa ne znači to što su ove tri različite funkcije najčešće sakupljene zajedno, te ih se naziva zajedničkim imenom **provjera autentičnosti**. Najjednostavnije rečeno, AH osigurava da vaši podaci nisu bili neovlašteno promijenjeni na putu do svog konačnog odredišta.

Iako AH radi provjeru autentičnosti IP datagrama u što je moguće većoj mjeri, primalac nije u mogućnosti predvidjeti vrijednosti određenih polja u IP zaglavlju. AH ne radi zaštitu ovih polja, poznatih kao **promjenljiva** 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*. Ovaj RFC možete pogledati na Internetu na sljedećoj Web stranici: <http://www.rfc-editor.org>



Načini korištenja AH protokola

AH možete primijeniti na dva načina: transportni način ili tunelski način. U transportnom načinu, IP zaglavlje datagrama je krajnje vanjsko IP zaglavlje, slijedi ga AH zaglavlje i zatim teret datagrama. AH provjerava autentičnost cijelog datagrama, osim promjenljivih polja. Ipak, informacije sadržane u datagramu transportirane su u razgovjetnom 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 datagrama. AH zaglavlje slijedi novo IP zaglavlje. Originalni datagram (oboje, IP zaglavlje i originalni teret) dolazi zadnji. AH radi provjeru autentičnosti cijelog datagrama, što znači da odgovarajući sistem može otkriti da li je datagram promijenjen za vrijeme prolaska.

Kada je bilo koji kraj sigurnosnog udruženja 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 regulirati da AH tunel provjeri autentičnost svog prometa između mreža koje povezuju. Zapravo, ovo je vrlo tipična konfiguracija.

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

Zašto AH?

U mnogim slučajevima vaši podaci zahtijevaju samo provjeru autentičnosti. Dok protokol Sažimanje tereta sigurnosti (ESP) može izvoditi provjeru autentičnosti, AH ne utječe na performanse vašeg sistema kao ESP. Druga prednost korištenja AH je to da AH provjerava autentičnost cijelog datagrama. 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. Jaka kriptografija u nekim je zemljama ograničena, dok AH nije reguliran i može biti slobodno korišten širom svijeta.

Koje algoritme AH koristi za zaštitu mojih informacija?

AH koristi algoritme poznate kao **kodovi za provjeru autentičnosti raspršenih poruka (HMAC)**. Specifično, VPN koristi ili HMAC-MD5, ili HMAC-SHA. Oba algoritma, MD5 i SHA, uzimaju ulazne podatke promjenljive dužine i tajni ključ da bi proizveli izlazne podatke fiksirane 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*. Ova dva RFC-a možete pogledati na Internetu na sljedećoj Web stranici: <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 Zaglavlje za provjeru autentičnosti (AH) je da u tome što ESP omogućuje šifriranje, dok oba protokola omogućuju provjeru autentičnosti, provjeru integriteta i zaštitu od ponovljenog izvođenja. 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 sa dešifriranjem. Ovaj tip konfiguracije smanjuje opterećenje kod obrade, te također smanjuje vašu ranjivost na napade tipa 'uskraćivanje 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 datagrama. Ako datagram 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 datagrami 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 datagrama, koje slijedi ESP zaglavlje i zatim originalni datagram (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 datagram, 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 ESP koristi za zaštitu mojih 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. OS/400^(R) VPN koristi za šifriranje Standard Šifriranja Podataka (DES), trostruki-DES (3DES), RC5, RC4 ili Napredni Standard Šifriranja (AES).

Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira DES u Zahtjevu za komentarima (RFC) 1829, *The ESP DES-CBC Pretvorba*. Jedinica za zadatke u Internet inženjeringu (IETF) službeno definira 3DES u RFC 1851, *ESP Trostruka DES Pretvorba*. Ovaj i ostale RFC-ove možete pogledati 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 promjenljive dužine i tajni ključ da bi proizveli izlazne podatke fiksirane 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*. Ovaj i ostale RFC-ove možete pogledati na Internetu na sljedećoj Web stranici: <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 datagram. Iako kombiniranje dva protokola nudi veću sigurnost, opterećenje uključeno pri obrađivanju može nadmašiti samu korist.

Upravljanje ključevima

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

VPN upravitelj ključeva je IBM^(TM)s implementacija protokola Internet razmjene ključeva (IKE). Upravitelj ključeva podržava automatsko pregovaranje sigurnosnih udruženja (SA), kao i automatsku generaciju i osvježavanje kriptografskih ključeva.

Sigurnosno udruženje (SA) sadržava 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.

Opaska: Sigurno generiranje vaših ključeva je najvažniji 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 netrivialan 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, koristeći Upravitelja digitalnih certifikata (5722-SS1 Opcija 34). Dodatno, neka VPN rješenja zahtijevaju RSA Potpis za

međuooperabilnost. Na primjer, Windows^(R) 2000 VPN koristi RSA Potpis kao svoj default način 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 sa 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.

Kada kreirate dinamički VPN korištenjem iSeries^(TM) Navigatora, morate definirati IKE politiku za omogućavanje pregovora faze 1 i politiku podataka za upravljanje pregovorima 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.

Predloženo čitanje

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, *Domena interpretacije Internet IP Sigurnosti za ISAKMP*
- RFC 2408, *Internet Sigurnosno udruženje i Protokol za upravljanje ključem (ISAKMP)*
- RFC 2409, *Internet razmjena ključa (IKE)*

Ove RFC-ove možete pogledati na Internetu na sljedećoj Web stranici: <http://www.rfc-editor.org>



Sloj 2 Tunelski Protokol (L2TP)

Sloj 2 Tunelski protokol (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 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 krajnoj točki. Kod dobrovoljnog tunela, tunel završava na udaljenom klijentu, dok prisilni tunel završava na ISP-u.

Sa L2TP **prisilnim tunelom**, udaljeni host započinje vezu na svog Dobavljača Internet usluga (ISP). ISP zatim uspostavlja L2TP vezu između udaljenog korisnika i korporativne mreže. Iako ISP uspostavlja vezu, vi odlučujete kako zaštititi promet kod korištenja VPN-a. Kod prisilnog tunela ISP mora podržavati L2TP.

Sa 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. Sa dobrovoljnim tunelom, ISP ne treba podržavati L2TP. scenarij, *Zaštita L2TP dobrovoljnog tunela s IPSec* pruža vam primjer kako konfigurirati iSeries^(TM) iz podružnice da se spoji na korporativnu mrežu preko prilaza iSeries s L2TP tunelom zaštićenim VPN-om.



Možete vidjeti vizualnu prezentaciju koncepta zaštite L2TP dobrovoljnog tunela s IPSec. Ovo zahtijeva da imate 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 datagrama (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.

Pogledajte Scenarij: Konfiguriranje udaljene PPP veze na biranje za primjer kako se L2TP koristi kod povezivanja na IBM^(R), preko Univerzalne veze.

Prijevod mrežne adrese za VPN

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 htjeti komunicirati s drugom mrežom, ali obje mreže koriste 10.*.* adrese, što uzrokuje sudaranje adresa i ispuštanje svih paketa. Primjena NAT-a na vaše odlazne adrese može izgledati kao rješenje vaših problema. Ipak, ako je promet podataka zaštićen od VPN-a, konvencionalni NAT neće raditi jer mijenja IP adrese u sigurnosnom udruženju (SA), a koje VPN zahtijeva za funkcioniranje. Da izbjegnute 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.

Opaska: FTP u ovom trenutku ne podržava VPN NAT.

Kako 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 izbjegnute 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 da li je vaš poslužitelj inicijator ili odzivnik za VPN vezu. Kada je vaš poslužitelj inicijator veze možete prevoditi vaše lokalne adrese u one koje su kompatibilne s adresom vašeg partnera kod VPN veze. Kada je vaš poslužitelj odzivnik na vezu, možete prevesti udaljene adrese vašeg VPN partnera u one koje su kompatibilne s vašom lokalnom shemom adresiranja. Konfigurirajte ovaj tip prijevoda adresa samo za vaše dinamičke veze.

VPN NAT za sakrivanje 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 se vaš poslužitelj ponaša kao odzivnik za svoje veze.

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

1. Da li imate jedan ili više poslužitelja na koji želite da ljudi pristupaju korištenjem 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, *Korištenje prijevoda mrežnih adresa (NAT) za VPN* vam daje primjer kako konfigurirati VPN NAT da skriva lokalne adrese na vašoj iSeries^(TM).

Za upute korak po korak kako postaviti VPN NAT na vašoj iSeries, poslužite se online sistemom pomoći koji je dostupan iz VPN sučelja u iSeries Navigatoru.

NAT kompatibilni IPSec

Problem: Konvencionalni NAT ruši 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 nevaljanim. Kada se to dogodi, kraj VPN veze koji je primalac odbacuje paket i pregovori za VPN vezu završavaju neuspjehom.

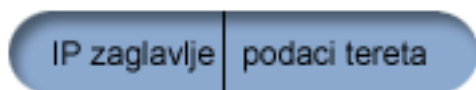
Rješenje: UDP sažimanje

U ljustici, 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.

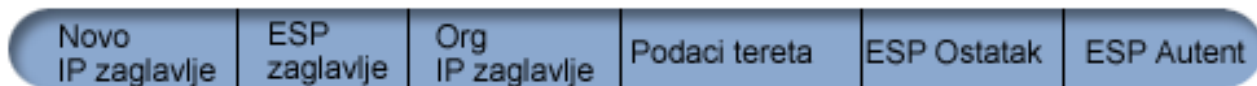
UDP sažimanje možete primijeniti samo na VPN-ove koji će koristiti IPSec ESP bilo u tunelskom ili transportnom načinu. Dodatno, od v5r2, iSeries^(TM) poslužitelj može raditi samo kao klijent za UDP sažimanje. Odnosno, on može samo *inicirati* UDP sažeti promet.

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

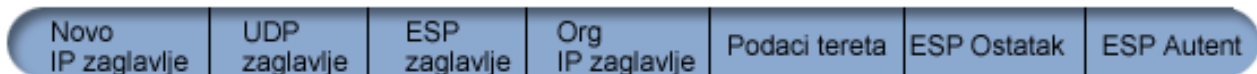
Originalni IPv4 datagram:



Nakon primjene IPSec ESP-a u tunelskom načinu:



Nakon primjene UDP sažimanja:

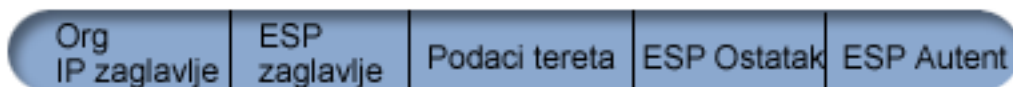


Donja grafika ilustrira format UDP sažetog ESP paketa u transportnom načinu:

Originalni IPv4 datagram:



Nakon primjene IPSec ESP-a u transportnom načinu:



Nakon primjene UDP sažimanja:



Jednom kad je paket sažet, iSeries šalje paket svojem VPN partneru preko UDP-a na portu 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 izvorišnjog 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 postavljene na nula u IKE paketu. Da bi sve ispravno radilo, oba kraja veze moraju podržavati UDP sažimanje.



IP komprimiranje (IPComp)

Protokol IP komprimiranja tereta (IPComp) smanjuje veličinu IP datagrama komprimiranjem datagrama 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)*. Ovaj RFC možete pogledati na Internetu na sljedećoj Web stranici: <http://www.rfc-editor.org>



VPN i IP filtriranje

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.

Počevši sa V5R1 verzijom operativnog sistema, VPN može automatski generirati ova pravila. Kada je god moguće, dozvolite VPN-u da generira za vas vaše filtere politika. Ne samo da će vam ovo pomoći da uklonite greške, nego će ukloniti potrebu da konfigurirate pravila kao dodatan korak koristeći editor Paketnih pravila u iSeries^(TM) Navigatoru.

Naravno, postoje i iznimke. Pregledajte ova poglavlja da više naučite o drugim, manje uobičajenim, konceptima i tehnikama VPN-a i filtriranja, koji se mogu primijeniti na vašu određenu situaciju:

- **Migracija filtera politika na trenutno izdanje**

Na V4R4 i V4R5 operativnom sistemu morali ste kao poseban korak konfigurirati VPN paketna pravila. Ona nisu

bila generirana automatski kao dio vaših VPN konfiguracija. Ovo poglavlje daje detalje posebnih razmatranja za migriranje V4R4 i V4R5 filtera politika na trenutno izdanje, te vam govori kako da to napravite.

- **VPN veza bez filtera politika**

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. Ovo poglavlje objašnjava zašto bi mogli razmotriti ovu mogućnost i daje naznake kako to napraviti.

- **Uključeni IKE**

Da bi se IKE pregovori desili za vaš VPN, trebate dozvoliti UDP datagrame preko porta 500 za ovaj tip IP prometa. Ipak, ako nema pravila filtriranja na sistemu specifično napisanih sa svrhom dozvole IKE prometa, tada će sistem uključivo dozvoliti protok IKE prometa. Pročitajte ovo poglavlje za više informacija kako to radi na iSeriesu.

Migracija filtera politika na trenutno izdanje

Na V4R4 i V4R5 operativnom sistemu morali ste kao poseban korak konfigurirati VPN paketna pravila u sučelju Pravila paketa u iSeries^(TM) Navigatoru. Ona nisu bila generirana automatski kao dio vaših VPN konfiguracija. Počevši sa V5R1 verzijom operativnog sistema, VPN GUI može automatski kreirati ova paketna pravila.

Nekoliko je stavki koje morate razmotriti ako ste kreirali pravila za filtriranje politika (pravila gdje je akcija=IPSec) u verziji V4R5 ili V4R5, a želite koristiti ta ista pravila i na trenutnom izdanju. Ili, možda *će* VPN generirati vaša pravila za filtriranje politika, ali vi trebate dodati dodatna pravila koja dozvoljavaju ostali IP promet; na primjer, telnet, preko cijele veze. Slijedite ove preporuke da vam pomognu izbjeći moguće greške u konfiguraciji.

Da razjasnimo: Kada se ovo poglavlje odnosi na datoteku pravila za *korisnika*, ono se odnosi na sva pravila koja ste kreirali koristeći editor Paketna pravila u iSeries Navigatoru. Suprotnost ovome je datoteka pravila *VPNPOLICYFILTERS.I3P*, koja je datoteka za pravila koja VPN automatski generira kao dio VPN konfiguracija.

- Ako imate VPN veze na jednoj od verzija, V4R4 ili V4R5 i ne planirate konfigurirati druge VPN veze u trenutnom izdanju, možete aktivirati vaša pravila za filtriranje i pokrenuti vaše veze na uobičajeni način.
- Ako imate VPN veze na jednoj od verzija, V4R4 ili V4R5 i planirate konfigurirati druge VPN veze u trenutnom izdanju, koristite čarobnjaka **Migracija filtera politike**. Čarobnjak uklanja filtere za politike iz datoteka za paketna pravila koje ste kreirali i umeće ekvivalentne filtere za politike u VPNPOLICYFILTERS.I3P, koji generira VPN. Da pristupite čarobnjaku, slijedite ove korake:
 1. U iSeries Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
 2. Desno kliknite na **Virtualno privatno umrežavanje** i izaberite **Migriraj filtere za politike**.
 3. Kada dovršite čarobnjaka, kliknite **Završetak**.
 4. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
- Ako je VPN generirao vaša pravila za filtriranje politike, ali trebate dodati neka ne-VPN pravila filtriranja, morate konfigurirati ova pravila korištenjem editora Paketna pravila u iSeries Navigatoru. Ako bilo koje od ovih ne-VPN pravila filtriranja treba doći prije VPN filtera, tada počnite njihova imena sa **PREIPSEC**. Na primjer, **PREIPSECMYRULES**. Ovo će pomoći sistemu da odredi redosljed po kojem će obrađivati vaša pravila filtera. Imena skupova svih drugih ne-VPN pravila moraju imati **PREIPSEC** prefiks. Na primjer, **MORERULES**.
- Uvijek dozvolite VPN-u da kreira vaša pravila filtera politika. Ipak, vaša ne-VPN pravila filtriranja moraju ostati u datoteci pravila za vašeg korisnika. Zapamtite, ako bilo koji od ovih ne-VPN filtera treba doći prije filtera za politike u datoteci za pravila VPNPOLICYFILTERS.I3P, trebate dodati **PREIPSEC** ispred imena skupa. Ovo osigurava da vaša pravila za korisnika i VPN pravila rade zajedno, kao što je i bila vaša namjera. Na primjer, VPN je generirao vaša pravila za filtriranje politike (VPN skupovi), ali vi ste dodali dodatna pravila (vaši skupovi) da dozvolite drugi IP promet preko cijele veze. Kada učitate pravila na vaš sistem, ona će biti poredana na sljedeći način:
 1. Vaši skupovi čija imena počinju sa **PREIPSEC**
 2. VPN skupovi čije ime počinje sa **PREIPSEC**
 3. VPN skupovi s **ACTION=IPSEC** (filteri za politike)
 4. Vaši skupovi s **ACTION=IPSEC** (filteri za politike)
 5. Vaši skupovi sa svim ostalim.
 6. VPN skupovi sa svim ostalim.

Provjerite datoteku EXPANDED.OUT da pogledate poredak spojenih izlaznih datoteka. EXPANDED.OUT je napisana u direktorij gdje je locirana vaša datoteka sa pravilima za korisnika.

- Koristeći iSeries Navigator, možete izabrati aktivaciju:
 - samo datoteke sa VPN generiranim pravilima, VPNPOLICYFILTERS.I3P
 - samo vaše datoteke sa pravilima za korisnika
 - oboje, VPN generirana pravila i vaša osobna datoteka pravila
- Aktivirajte vaša pravila filtriranja na svim sučeljima, radije nego po pojedinačnom sučelju. Ovo pomaže u jamstvu da će filteri aktivirati i također postaviti ispravan poredak filtera za politike.
- Uvijek provjerite vaša pravila filtera prije nego ih pokušate aktivirati. Ako provjera prođe bez grešaka, provjerite EXPANDED.OUT zbog osiguranja da su pravila poredana kako ste namjeravali. Nakon što dovršite ovaj korak, možete aktivirati pravila.

VPN veze bez filtera politike

Filter politike definira koje adrese, protokoli i portovi mogu koristiti VPN i usmjerava prikladan promet preko te veze. U nekim slučajevima možda ćete htjeti konfigurirati vezu koja ne zahtijeva pravilo filtriranja politike. Na primjer, možda imate učitana ne-VPN paketa pravila na sučelju koje će koristiti vaša VPN veza i zato radije nego da deaktivirate aktivna pravila na tom sučelju, odlučili ste konfigurirati VPN tako da vaš sistem dinamički upravlja svim filterima 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 može biti inicirana samo od strane lokalnog poslužitelja.
- Krajnje točke podataka za vezu moraju biti jednostruki sistemi. To znači, one ne mogu biti pod mreža 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 paketa pravila učitana na vaš sistem.

Za upute korak po korak kako konfigurirati vezu tako da ne zahtijeva filter politike, poslužite se online sistemom pomoći za VPN.

Uključeni IKE

Za uspostavu veze, većina VPN-ova zahtijeva da se pregovori Internet razmjene ključeva (IKE) dese prije nego se može desiti obrada IPSec. IKE koristi dobro poznati port 500. Zato, da bi IKE radio ispravno, trebate dozvoliti UDP datagrame 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.

Plan za VPN

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 da sakupite sve informacije koje trebate da osigurate da je vaš VPN uspješan:

- **Zahtjevi za VPN postav**
Prije nego počnete, osigurajte da udovoljavate minimalnim zahtjevima za kreiranje VPN-a.
- **Odredite koji tip VPN-a kreirati**
Određivanje kako ćete koristiti vaš VPN jedan je od prvih koraka u uspješnom planiranju. Ovo poglavlje opisuje različite tipove veza koje možete konfigurirati.
- **Koristi savjetnik za VPN planiranje**
Savjetnik za planiranje vas ispituje o vašoj mreži i na osnovu vaših odgovora daje vam prijedloge za kreiranje vašeg VPN-a.
Opaska: Koristite savjetnik za VPN planiranje samo za veze koje podržavaju protokol Internet razmjene ključa (IKE). Koristite radnu tablicu za planiranje ručnih veza za vaše tipove ručnih veza.

- **Popunite radne tablice za planiranje VPN-a**

Ako preferirate, možete ispisati i popuniti radne tablice za planiranje VPN-a da sakupite detaljne informacije o planovima upotrebe vašeg VPN-a.

Nakon što isplanirate postavljanje vašeg VPN-a, možete započeti sa njegovom konfiguracijom.

Zahtjevi za VPN postav

Za pravilno funkcioniranje na iSeries^(TM) te sa mrežnim klijentima osigurajte da vaša iSeries i klijentski PC udovoljavaju slijedećim zahtjevima:

V5R2 iSeries zahtjevi

- OS/400^(R) Verzije 5 Izdanja 2 (5722-SS1) ili kasniji
- Upravitelj digitalnih certifikata (5722-SS1 Opcija 34)
- Dobavljač kriptografičkog pristupa (5722-AC2 ili AC3)
- iSeries Access for Windows^(R)(5722-XE1) i iSeries Navigator
 - Komponenta Mreža iSeries Navigatora
- 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^(R) 32-bitnim operacijskim sistemom ispravno vezanim za vašu iSeries i konfiguriranom za TCP/IP
- A 233 Mhz jedinica za obradu
- 32 MB RAM za Windows 95/98 klijente
- 64 MB RAM za Windows NT^(R) i 2000 klijente
- iSeries Access za Windows i iSeries Navigator instaliran na PC klijenta
- Softver koji podržava protokol IP Sigurnost (IPSec)
- Softver koji podržava L2TP, ako udaljeni korisnici koriste L2TP za uspostavljanje veze sa vašim sistemom

Određivanje tipa VPN-a za kreiranje

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 su krajnje točke *veze* različite 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, te 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 Sigurnost (IPSec) štiti promet dok putuje između dva prilaza. Ipak, IPSec ne štiti promet podataka niti na jednoj strani dva prilaza unutar internih mreža. Ovo je uobičajeni postav za veze između grana ureda, jer promet koji je usmjeren dalje od prilaza grana ureda, unutar interne mreže, je najčešće smatran pouzdanom.

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.

Popunjavanje radnih tablica za planiranje VPN-a

Koristite radne tablice za planiranje VPN-a da sakupite detaljne informacije o planovima upotrebe vašeg VPN-a. Ove informacije trebate da primjereno isplanirate vašu VPN strategiju. Ove informacije možete također koristiti da konfigurirate vaš VPN. Izaberite radnu tablicu za tip veze koju želite kreirati.

- **Radna tablica za planiranje dinamičkih veza**

Popunite ovu radnu tablicu prije nego konfigurirate dinamičku vezu.

- **Radna tablica za planiranje ručnih veza**

Popunite ovu radnu tablicu prije nego konfigurirate ručnu vezu.

- **Savjetnik za planiranje VPN-a**

Ili, ako preferirate, 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.

Opaska: Koristite savjetnik za planiranje VPN-a samo za vaše dinamičke veze. Koristite radnu tablicu za planiranje ručnih veza za vaše tipove ručnih veza.

Ako ćete kreirati višestruke veze sa sličnim svojstvima, možda ćete htjeti postaviti VPN default vrijednosti. 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**.

Radna tablica za planiranje za dinamičke veze

Prije nego kreirate vaše dinamičke VPN veze, popunite ovu radnu tablicu. Radna tablica pretpostavlja da ćete koristiti Čarobnjaka za novu vezu. Čarobnjak vam dozvoljava da postavite VPN na osnovu vaših osnovnih zahtjeva sigurnosti. U nekim slučajevima možda ćete trebati poboljšati svojstva koja čarobnjak konfigurira za vezu. Na primjer, možda odlučite da vam je potrebno vođenje dnevnika, ili da želite da se VPN poslužitelj pokrene svaki put kada se pokrene TCP/IP. 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.

Kontrolna lista preduvjeta	Odgovori
Da li je vaš OS/400 ^(R) V5R2 (5722-SS1) ili kasniji?	
Da li je instalirana opcija Upravitelj digitalnih certifikata (5722-SS1 Opcija 34)?	
Da li je instaliran Dobavljač kriptografičkog pristupa (5722-AC2 ili AC3)?	
Da li je instaliran iSeries ^(TM) Access (5722-XE1)?	
Da li je instaliran iSeries Navigator?	

Kontrolna lista preduvjeta	Odgovori
Da li je instalirana podkomponenta Mreža od iSeries Navigatora?	
Da li je instaliran Pomoćni program za TCP/IP povezanost za OS/400 (5722-TC1)?	
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	
Da li je TCP/IP konfiguriran na vašem iSeries (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 vatreni zid ili usmjerivače koji koriste IP filtriranje da li pravila filtriranja vatrene zida ili usmjerivača podržavaju AH i ESP protokole?	
Da li su vatreni zidovi ili usmjerivači konfigurirani da dozvole IKE (UDP port 500), AH i ESP protokole?	
Da li su vatreni zidovi konfigurirani da omoguće IP prosljeđivanje?	

Ove informacije trebate za konfiguraciju dinamičke VPN veze	Odgovori
Koji tip veze kreirate? <ul style="list-style-type: none"> • 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? <ul style="list-style-type: none"> • Najviša sigurnost, najniža izvedba • Uravnoteženu sigurnost i izvedbu • 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 ključeva?	
Koji je identifikator za lokalnu krajnju točku podataka?	
Koji je identifikator udaljenog poslužitelja ključeva?	
Koji je identifikator za udaljenu krajnju točku podataka?	
Koji tip sigurnosti i izvedbe sistema trebate za zaštitu vaših podataka? <ul style="list-style-type: none"> • Najviša sigurnost, najniža izvedba • Uravnoteženu sigurnost i izvedbu • Najniža sigurnost i najviša izvedba 	

Radna tablica za planiranje za ručne veze

Popunite ovu radnu tablicu koja će vam pomoći u kreiranju vaših veza virtualne privatne mreže (VPN) koje ne koriste IKE za upravljanje ključevima.

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

Kontrolna lista preduvjeta	Odgovori
Da li je vaš OS/400 ^(R) V5R2 (5722-SS1) ili kasniji?	
Da li je instalirana opcija Upravitelj digitalnih certifikata (5722-SS1 Opcija 34)?	

Kontrolna lista preduvjeta	Odgovori
Da li je instaliran Dobavljač kriptografičkog pristupa (5722-AC2 ili AC3)?	
Da li je instaliran iSeries ^(TM) Access (5722-XE1)?	
Da li je instaliran iSeries Navigator?	
Da li je instalirana podkomponenta Mreža od iSeries Navigatora?	
Da li je instaliran Pomoćni program za TCP/IP povezanost za OS/400 (5722-TC1)?	
Da li ste postavili sistemsku vrijednost za zadržavanje sigurnosnih podataka poslužitelja (QRETSVRSEC *SEC) na 1?	
Da li je TCP/IP konfiguriran na vašem iSeries (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 vatreni zid ili usmjerivače koji koriste IP filtriranje da li pravila filtriranja vatrene zida ili usmjerivača podržavaju AH i ESP protokole?	
Da li su vatreni zidovi ili usmjerivači konfigurirani da dozvole AH i ESP protokole?	
Da li su vatreni zidovi konfigurirani da omoguće IP prosljeđivanje?	

Ove informacije trebate za konfiguraciju ručne VPN veze	Odgovori
Koji tip veze kreirate? <ul style="list-style-type: none"> • 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 za VPN za više informacija.	
Da li ćete koristiti tunelski ili transportni način?	
Koji će IPSec protokol veza koristiti (AH, ESP, ili AH sa 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)?	
Opaska: Algoritam za šifriranje navodite samo ako ste izabrali ESP kao vaš 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.	

Ove informacije trebate za konfiguraciju ručne VPN veze	Odgovori
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.	

Konfiguriranje VPN-a

VPN sučelje vam omogućava nekoliko različitih načina za konfiguriranje vaših VPN veza. Nastavite čitati za pomoć oko odluke koji tip veze konfigurirati i kako to napraviti.

Koji tip veze trebam konfigurirati?

Dinamička veza je ona koja, dok je aktivna, dinamički generira i pregovara ključeve koji osiguravaju vašu vezu, korištenjem protokola Internet razmjene ključa (IKE). Dinamičke veze dobivaju 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.

Ručna (stranica 36) veza, međutim, ne pruža podršku za IKE pregovore i samim time automatsko upravljanje ključem. 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 ovo smatrate sigurnosnim rizikom, možda ćete ipak htjeti kreirati dinamičku vezu.

Kako konfiguriram dinamičku VPN vezu?

VPN je zapravo grupa konfiguracijskih objekata koja definira osobine veze. Dinamička VPN veza zahtijeva da svaki od ovih objekata radi ispravno. Slijedite niže navedene veze za određene informacije o tome kako konfigurirati svaki od VPN objekata:

Savjet:

Konfiguriranje veze pomoću Čarobnjaka za nove veze

Općenito, možete koristiti čarobnjaka Veze za kreiranje svih vaših dinamičkih veza. Čarobnjak automatski kreira svaki od konfiguracijskih objekata koje VPN zahtijeva za ispravan rad, uključujući i paketna pravila. Ako navedete da želite da čarobnjak aktivira VPN paketna pravila za vas, prijedite odmah na niže navedeni korak šest, *Pokreni vezu*. U suprotnom, nakon što čarobnjak završi konfiguriranje vašeg VPN-a, morate aktivirati paketna pravila i zatim možete pokrenuti vezu.

Ako izaberete da ne koristite čarobnjaka za konfiguriranje vaših dinamičkih VPN veza, slijedite ove korake za dovršetak konfiguracije:

1. Konfiguriranje VPN politika sigurnosti

Morate definirati VPN politike sigurnosti za sve vaše dinamičke veze. Politika Internet razmjene ključa i politika podataka određuju kako IKE štiti svoje pregovore faze 1 i faze 2.

2. Konfiguriranje sigurne veze

Jednom kad ste definirali politike sigurnosti za 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, dok **veza dinamičkog ključa** definira karakteristike pojedinačnih veza podataka između parova krajnjih točaka. Veza dinamičkog ključa postoji unutar grupe dinamičkog ključa.

Opaska: Potrebno je dovršiti samo sljedeća dva koraka, *Konfiguriraj paketna pravila* i *Definiraj sučelje za pravila*, ako izaberete opciju **Pravila filtriranja politike će biti definirana u Paketnim pravilima** na stranici **Grupa dinamičkog ključa - Veze** na VPN sučelju. Inače, ova pravila se kreiraju kao dio vaše VPN konfiguracije i primjenjuju se na sučelje koje specificirate.

Preporuča se da uvijek dozvolite VPN sučelju da kreira vaša pravila filtriranja politike za vas. To napravite izborom opcije **Generiraj sljedeći filter politike za ovu grupu** na stranici **Grupa dinamičkog ključa - Veze**.

3. Konfiguriranje paketnih pravila

Nakon što dovršite vaše VPN konfiguracije, morate kreirati i primijeniti pravila filtriranja da dozvolite promet podataka da protječe kroz vezu. VPN **pred-IPSec** pravila dozvoljavaju ukupan IKE promet na navedenim sučeljima tako da IKE može pregovarati veze. Pravilo **filtriranja politike** definira koje adrese, protokole i portove može koristiti pridružena nova grupa dinamičkog ključa.

Ako migrirate sa bilo V4R4 ili V4R5 i imate VPN veze i filtere politika koje želite nastaviti koristiti s trenutnim izdanjem, pogledajte temu *Migracija filtera politika na trenutno izdanje* za osiguranje da vaši stari filteri politika i novi filteri politika rade zajedno kao što vam je i bila namjera.

4. Definiranje sučelja za pravila

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

5. Aktiviranje paketnih pravila

Nakon što definirate sučelje za vašu paketna pravila, morate ih aktivirati prije nego možete pokrenuti vezu.

6. Pokretanje veze

Dovršite ovaj zadatak da pokrenete vaše veze.

Kako konfiguriram ručnu VPN vezu?

Kao što samo ime sugerira, ručna veza je ona gdje morate konfigurirati sva vaša VPN svojstva ručno, uključujući ulazne i vanjske ključeve. Slijedite niže navedene veze za određene informacije o tome kako konfigurirati ručnu vezu:

1. Konfiguriranje ručne veze

Ručne veze definiraju karakteristike veze, uključujući sigurnosne protokole i krajnje točke veze i podataka.

Opaska: Potrebno je dovršiti samo sljedeća dva koraka, *Konfiguriraj pravilo filtriranja politike* i *Definiraj sučelje za pravila*, ako izaberete opciju **Pravilo filtriranja politike će biti definirano u Paketnim pravilima** na stranici **Ručna veza - Veze** na VPN sučelju. Inače, ova pravila se kreiraju kao dio vaših VPN konfiguracija.

Preporuča se da uvijek dozvolite VPN sučelju da kreira vaša pravila filtriranja politike za vas. To napravite izborom opcije **Generiranje filtera politike koji se podudara sa krajnjim točkama podataka** na stranici **Ručna veza - Veza**.

2. Konfiguriranje pravila filtriranja politike

Nakon što konfigurirate atribut za ručnu vezu, morate kreirati i primijeniti pravilo filtriranja politike koje dozvoljava prometu podataka da protječe kroz vezu. Pravilo **filtriranja politike** definira koje adrese, protokole i portove može koristiti pridružena veza.

3. Definiranje sučelja za pravila

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

4. Aktiviranje paketnih pravila

Nakon što definirate sučelje za vašu paketna pravila, morate ih aktivirati prije nego možete pokrenuti vezu.

5. Pokretanje veze

Dovršite ovaj zadatak da pokrenete veze koje su započete lokalno.

Konfiguriranje VPN veze pomoću Čarobnjaka za 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. Ipak, ako trebati dodati funkciju vašem VPN-u; na primjer, vođenje dnevnika ili prijevod mrežne adrese za VPN (VPN NAT), možda ćete htjeti dalje poboljšati vaš VPN preko listova svojstava za prikladnu grupu 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**.

Prije nego započnete popunite Savjetnik za planiranje VPN-a. 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 iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** vašeg poslužitelja.
2. Desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Nova veza** da započnete Čarobnjaka.
3. Dovršite čarobnjaka da kreirate osnovnu VPN vezu. Kliknite **Pomoć** ako zatrebate pomoć.

Konfiguriranje VPN politika sigurnosti

Nakon što odredite kako ćete koristiti vaš VPN, morate definirati vaše politike VPN sigurnosti. Specifično, vi trebate:

- **Konfiguriranje politike Internet razmjene ključeva (IKE)**
IKE politika definira koju razinu provjere autentičnosti i zaštite šifriranja IKE koristi za vrijeme pregovora faze 1. 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.
- **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.

Nakon što konfigurirate vaše politike za VPN sigurnost, morate konfigurirati sigurne veze.

Konfiguriranje politike Internet razmjene ključeva (IKE)

IKE politika definira koju razinu provjere autentičnosti i zaštite šifriranja IKE koristi za vrijeme pregovora faze 1. IKE faza 1 uspostavlja ključeve koji štite poruke koje protječu u pregovore sljedeće faze 2. VPN koristi ili RSA način potpisa, ili unaprijed podijeljeni ključ za provjeru autentičnosti pregovora faze 1. Ako planirate koristiti digitalne certifikate za provjeru autentičnosti poslužitelja ključeva, morate ih najprije konfigurirati korištenjem Upravitelja digitalnih certifikata (5722-SS1 Opcija 34). 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 iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Politike IP sigurnosti** vašeg poslužitelja.
2. Da kreirate novu politiku, desno kliknite **Politike Internet razmjene ključeva** i izaberite **Nova politika Internet razmjene ključeva**. 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 o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** da spremite vaše promjene.



Opaska: Preporučljivo je da koristite glavni način pregovaranja kad god se dijeljeni ključ koristi za provjeru autentičnosti. On pruža 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 lozinke. Također se preporučuje da periodički mijenjate vaše lozinke. Koristite online sistem pomoći iSeries Navigatora za više detaljnih informacija.



Konfiguriranje politike podataka

Politika podataka definira koja razina provjere autentičnosti ili šifriranja štiti podatke dok protječu kroz VPN. Komunikacijski sistemi se slažu nad ovim atributima za vrijeme protokola Internet razmjena ključa (IKE) pregovora faze 2.

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Politike IP sigurnosti** vašeg poslužitelja.
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 **Svojtva**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** da spremite vaše promjene.

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.

Da konfigurirate objekt sigurne veze, dovršite ove zadatke:

Dio 1: Konfiguriranje grupe dinamičkog ključa:

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Desno kliknite **Po grupi** i izaberite **Nova grupa dinamičkog ključa**.
3. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** da spremite vaše promjene.

Dio 2: Konfiguriranje veze dinamičkog ključa:

1. U iSeries Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** → **Po grupi** vašeg poslužitelja.

2. U lijevom oknu prozora iSeries Navigatora desno kliknite na grupu dinamičkog ključa koju ste kreirali u prvom dijelu i izaberite **Nova veza dinamičkog ključa**.
3. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** da spremite vaše promjene.

Nakon što dovršite ove korake, trebate aktivirati paketna pravila koja veza zahtijeva za pravilan rad.

Opaska: U većini slučajeva, dozvolite VPN sučelju da automatski kreira vaša VPN pravila paketa izborom opcije **Generiraj sljedeći filter politike za ovu grupu** na stranici **Grupa dinamičkog ključa - Veze**. Ipak, ako izaberete opciju **Pravilo filtriranja politike biti će definirano u paketnim pravilima**, morate zatim konfigurirati VPN paketna pravila korištenjem editora Paketna pravila, a zatim ih aktivirati.

Konfiguriranje ručne veze

Kao što samo ime sugerira, ručna veza je ona gdje morate konfigurirati sva vaša VPN svojstva ručno. 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 ovo smatrate sigurnosnim rizikom, a oba kraja veze podržavaju protokol Internet razmjene ključeva (IKE), možda ćete umjesto toga htjeti razmotriti postavljanje dinamičke veze.

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Desno kliknite na **Sve veze** i izaberite **Nova ručna veza**.
3. Ispunite svaki od listova svojstava. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** da spremite vaše promjene.

Opaska: U većini slučajeva, dozvolite da vam VPN sučelje automatski generira VPN pravila paketa izborom opcije **Generiranje filtera politike koji se podudara sa krajnjim točkama podataka** na stranici **Ručna veza - Veza**. Ipak, ako izaberete opciju **Pravilo filtriranja politike biti će definirano u paketnim pravilima**, morate zatim ručno konfigurirati pravila filtriranja politike, a zatim ih aktivirati.

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 vlastita pravila VPN paketa koristeći editor Paketnih pravila u iSeries^(TM) Navigatoru, kreirajte bilo koja druga pravila na isti 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 poglavlje niže da naučite kako konfigurirati ova pravila korištenjem editora Paketna pravila u iSeries Navigatoru. Ako želite pročitati o drugim VPN i filterskim opcijama, pogledajte *VPN i IP filtriranje* odlomak poglavlja VPN koncepti.

- **Pred-IPSec pravila**

Pred-IPSec pravila su bila 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 politici sigurnosti.

Opaska: Trebate konfigurirati samo ovaj tip pred-IPSec pravila ako već imate druga pravila koja dozvoljavaju IKE za određene sisteme. Ako nema pravila filtriranja na sistemu napisanih sa svrhom dozvole IKE prometa, tada je IKE promet uključeno dozvoljen.

- **Pravilo filtriranja politike**

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

Stvari koje treba razmotriti prije nego započnete

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 možete otkriti da promet koji je prethodno radio zagonetno ne uspijeva nakon što aktivirate vaša VPN pravila filtriranja. Ako na sučelju želite dozvoliti promet različit od VPN-a, morate dodati izričita PERMIT pravila.

Nakon što konfigurirate prikladna pravila filtriranja, morate definirati sučelje na koje se odnose, a zatim ih aktivirati.

Od velike je važnosti da ispravno konfigurirate vaša pravila filtriranja. Ako to ne napravite, pravila filtriranja mogu blokirati sav IP promet koji dolazi i odlazi sa vašeg iSeries poslužitelja. To uključuje vašu vezu na iSeries Navigator, koju koristite za konfiguriranje pravila filtriranja.

Ako pravila filtriranja ne dozvole promet iSeries Navigatora, iSeries Navigator ne može komunicirati s vašim iSeriesom. Ako se nađete u ovoj situaciji, morate se prijaviti na vaš iSeries koristeći sučelje koje još uvijek ima vezu, 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.

Konfiguriranje pred-IPSec pravila filtriranja

Pažnja: Dovršite ovaj zadatak samo ukoliko ste naveli da ne želite da VPN automatski kreira pravila vašeg 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 datagrame 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 iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Paketna pravila** i izaberite **Editor pravila**. Ovo otvara editor Paketna pravila, što vam dozvoljava da kreirate ili uredite filter i NAT pravila za vaš iSeries.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Paketna pravila 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 **Servisi** izaberite **Servis**. 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.

Opaska: Manje sigurna, ali jednostavnija opcija za dozvolu IKE prometa preko veze je konfiguriranje samo jednog pred-IPSec filtera i upotreba vrijednosti zamjenskog znaka (*) u poljima **Smjer**, **Ime adrese izvora** i **Ime adrese odredišta**.

Sljedeći korak je konfiguriranje pravila filtriranja politike da definirate koji IP promet VPN veza štiti.

Konfiguriranje pravila filtriranja politike

Pažnja: Dovršite ovaj zadatak samo ukoliko ste naveli da ne želite da VPN automatski kreira pravila vašeg 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:

Opaska: Ako ste upravo konfigurirali pre-IPSec pravilo (samo za dinamičke veze) editor Pravila paketa će još uvijek biti otvoren; idite na korak četiri.

1. U iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Paketna pravila** i izaberite **Editor pravila**. Ovo otvara editor Paketna pravila, što vam dozvoljava da kreirate ili uredite filter i NAT pravila za vaš iSeries.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Paketna pravila 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. (neobvezno) 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 je korak definiranje sučelja na koje se odnose ova pravila filtriranja.

Opaska: Kada dodate pravila filtriranja za sučelje, sistem automatski dodaje default DENY pravilo za sučelje. To znači da je zabranjen bilo kakav promet koji izričito nije dozvoljen. Ovo pravilo ne možete vidjeti ili mijenjati. Kao rezultat možete otkriti da veze koje su prethodno radile zagonetno ne uspijevaju nakon što aktivirate vaša VPN paketna pravila. Ako na sučelju želite dozvoliti promet različit od VPN-a, morate dodati izričita PERMIT pravila.

Definiranje sučelja za VPN pravila filtriranja

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:

Opaska: Ako ste upravo konfigurirali VPN pravila paketa, sučelje Pravila paketa će još uvijek biti otvoreno; idite na korak četiri.

1. U iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Paketna pravila** i izaberite **Editor pravila**. Ovo otvara editor Paketna pravila, što vam dozvoljava da kreirate ili uredite filter i NAT pravila za vaš iSeries.
3. Na pozdravnom prozoru, izaberite **Kreiranje nove datoteke pravila paketa** i kliknite na **OK**.
4. Iz editora Paketna pravila izaberite **Umetni** —> **Sučelje za filtriranje**.
5. Na stranici **Općenito** izaberite **Ime linije**, zatim iz padajuće liste izaberite opis linije na koju se vaša VPN paketna pravila primjenjuju.
6. (neobvezno) 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 iSeries poslužitelju, s ekstenzijom .i3p.
Opaska: Ne spremajte vašu 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 filtriranja, morate ih aktivirati prije nego možete pokrenuti VPN.

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 zamjeniti.

ako odlučite aktivirati vaša VPN generirana pravila koristeći Editor pravila paketa, slijedite ove korake:

1. U iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Paketna pravila** i izaberite **Aktiviraj**. Ovo otvara kućicu dijaloga **Aktiviranje pravila paketa**.
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 što aktivirate vaša pravila filtriranja, možete pokrenuti vašu VPN vezu.

Pokretanje VPN veze

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

1. U iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Ako VPN poslužitelj nije pokrenut, desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Pokreni**. Ovo pokreće VPN poslužitelj.
3. Osigurajte da su vaša paketna pravila aktivirana.
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**.

Upravljanje s VPN-om

Koristite VPN sučelje u iSeries^(TM) Navigatoru za rukovanje svim upravljačkim zadacima, uključujući:

- **Pokreni VPN vezu**
Dovršite ovaj zadatak da pokrenete veze koje ćete započeti lokalno.
- **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 vijekove ključeva i životne vijekove veza.
- **Resetiraj veze u stanju greške**
Resetiranje veza s greškom vraća ih u stanje mirovanja.
- **Pogled na informacije o greški**
Ispunite ovaj zadatak za pomoć u određivanju zašto je vaša veza u stanju greške.
- **Pogledaj atribute aktivnih veza**
Ispunite ovaj zadatak da provjerite status i ostale atribute vaših aktivnih veza.
- **Koristi praćenje VPN poslužitelja**
Praćenje VPN poslužitelja vam dozvoljava da konfigurirate, pokrenete i pogledate praćenja poslužitelja za Upravitelja VPN veze i Upravitelja VPN ključa. Ovo je slično korištenju TRCTCPAPP *VPN naredbe iz znakovnog sučelja osim što možete gledati praćenje dok je veza aktivna.
- **Pogled na dnevnike poslova VPN poslužitelja**
Slijedite ove upute da pogledate dnevnike poslova za Upravitelja VPN ključa i Upravitelja VPN veze.
- **Zaustavi veze**
Dovršite ovaj zadatak da zaustavite aktivne veze.
- **Pogled na atribute Sigurnosnih udruženja (SA)**
Dovršite ovaj zadatak da prikazete atribute Sigurnosnih udruženja (SA) koji su pridruženi omogućenoj vezi.
- **Brisanje objekata VPN konfiguracije**
Prije nego obrišete objekat VPN konfiguracije iz baze podataka VPN politika, uvjerite se da razumijete kako to utječe na ostale VPN veze i grupe veza.

Postavljanje default atributa za vaše veze

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 iSeries^(TM) Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite **Virtualno privatno umrežavanje** i izaberite **Defaulti**.
3. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.
4. Kliknite **OK** nakon što ste dovršili svaki od listova svojstava.

Resetiranje veze u stanju greške

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
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**.

Pogled na informacije o greškama

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
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**.

Pogled na atribute aktivnih veza

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite na aktivnu vezu ili vezu na-zahtjev koju želite pogledati i izaberite **Svojstva**.
4. Otiđite na stranicu **Trenutni atributi** da pogledate atribute veze.

Također, možete pogledati atribute za sve veze iz prozora iSeries 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 iSeries Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Iz izbornika **Objekti** izaberite **Stupci**. Ovo otvara kućicu dijaloga koja vam omogućuje izbor atributa koje želite prikazati u prozoru iSeries Navigatora.

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

Upotreba praćenja VPN poslužitelja

Da pogledate praćenje VPN poslužitelja, slijedite ove korake:

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** vašeg poslužitelja.
2. Desno kliknite **Virtualno Privatno Umrežavanje**, izaberite **Alati za dijagnostiku**, a zatim **Praćenje poslužitelja**.

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

1. Iz prozora **Praćenje Virtualnog privatnog umrežavanja** kliknite



(Opcije).

2. Na stranici **Upravitelj veze** navedite koji tip praćenja želite da izvodi poslužitelj Upravitelj veze.
3. Na stranici **Upravitelj ključa** navedite koji tip praćenja želite da izvodi poslužitelj Upravitelj ključa.
4. Kliknite **Pomoć** ako imate pitanja o tome kako popuniti stranicu, ili bilo koje od njenih polja.

5. Kliknite **OK** da spremite vaše promjene.
6. Kliknite



(Pokreni) da pokrenete praćenje. Povremeno kliknite



(Osvježi) da pogledate posljednje informacije praćenja.

Pogled na dnevnik poslova VPN poslužitelja

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** vašeg poslužitelja.
2. Desno kliknite na **Virtualno Privatno Umrežavanje** i izaberite **Alati za dijagnostiku**, a zatim izaberite dnevnik posla koji želite pogledati.

Pogled na atribute Sigurnosnih udruženja (SA)

Da pogledate atribute sigurnosnih udruženja (SA) koji su pridruženi omogućenoj vezi. Da to napravite, slijedite ove korake:

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Kliknite **Sve veze** za prikaz popisa svih veza u desnom oknu.
3. Desno kliknite prikladnu aktivnu vezu i izaberite **Sigurnosna udruženja**. Rezultirajući prozor vam dozvoljava da pogledate svojstva svakog od SA-ova pridruženih određenoj vezi.

Zaustavljanje VPN veze

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
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

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

1. U iSeries^(TM) Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
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

VPN je kompleksna i brzo mijenjajuća tehnologija koja zahtijeva barem osnovno znanje standardnih IPSec tehnologija. Morate također biti upoznati sa pravilima IP paketa jer VPN zahtijeva nekoliko pravila filtera kako bi ispravno radio. Zbog ove kompleksnosti s vremena na vrijeme možete iskusiti probleme s vašim VPN vezama. Uklanjanje pogreške 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 daju vam savjete kako ukloniti pogreške kod različitih problema na koje možete naići kod korištenja VPN-a:

- **Započnite sa uklanjanjem pogreške VPN-a**

Otiđite ovdje da započnete pronalazak i ispravak vaših problema sa VPN vezom.

- **Najčešće greške VPN konfiguracije i kako ih popraviti**
Ovo poglavlje identificira najčešće korisničke greške i daje moguća rješenja.
- **Uklanjanje pogreške VPN-a sa QIPFILTER dnevnikom**
Ovo poglavlje daje informacije o vašim pravilima VPN filtriranja.
- **Uklanjanje pogreške VPN-a sa QVPN dnevnikom**
Ovo poglavlje daje informacije o IP prometu i vezama.
- **Uklanjanje pogreške VPN-a sa dnevnici poslova VPN-a**
Ovo poglavlje opisuje različite dnevnike poslova koje VPN koristi.
- **Rješavanje VPN problema s OS/400^(R) praćenjem komunikacije**
Ovo poglavlje opisuje kako pratiti podatke na komunikacijskoj liniji.

Kako započeti rješavanje problema VPN-a

Nekoliko je načina za početak analiziranja VPN problema:

1. Uvijek provjerite da ste primijenili zadnje Privremene popravke za program (PTF).
2. Osigurajte da ispunjavate minimum Zahtjeva za VPN postav.
3. Pregledajte sve poruke greške koje se nalaze u prozoru Informacije o greškama, ili Dnevnici poslova VPN poslužitelja, za oboje, lokalne i udaljene poslužitelje. 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 greška poruke koju pronađete ne pruža dovoljno informacija za rješavanje problema, provjerite dnevnik IP filter.
5. Praćenje komunikacija na iSeries^(TM) pruža još jedan način za pronalazak općenitih informacija 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^(R) Servis koristi TRCTCPAPP za pribavljanje izlaza praćenja da bi analizirao problem veze.

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 neka osnovna uputstva o tome kako započeti analizu VPN problema, od najjednostavnije IP veze do kompleksnije 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 sa lokalnog na udaljeni host?

Opaska: Imajte na umu prompt PING naredbe; unesite adresu udaljenog sistema i koristite PF10 za dodatne parametre, tada 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 sa 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.

Opaska: Moguće je da postoje posredni usmjerivači ili vatreni zidovi koji čine filtriranje IP paketa, te možda filtriraju i PING pakete. PING je uobičajeno zasnovan na ICMP protokolu. Ako je PING uspješan, znate da imate povezanost. Ako je PING neuspješan, znate samo da PING nije uspio. Možda ćete htjeti pokušati druge IP protokole između dva sistema, kao što su Telnet ili FTP, da provjerite povezanost.

2. Provjerite pravila filtriranja za VPN i osigurajte da su aktivirana. Da li je pokretanje filtriranja uspješno? Ako odgovorite **da**, tada nastavite sa korakom 3. Ako odgovorite **ne**, tada provjerite poruke greške u prozoru Paketna pravila u iSeries Navigatoru. Osigurajte da pravila filtriranja ne navode Prijevod mrežne adrese (NAT) za bilo koji VPN promet.

3. Pokrenite vašu VPN vezu. Da li je pokretanje veze uspješno? Ako odgovorite **da**, tada nastavite sa korakom 4. Ako odgovorite **ne**, tada provjerite od grešaka dnevnik posla QTOVMAN i dnevnik 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

Ovaj odlomak opisuje neke od najčešćih problema koji se pojavljuju kod VPN-a i povezuje vas na savjete o tome kako ih riješiti.

Opaska: Kada konfigurirate VPN, vi zapravo kreirate nekoliko različitih konfiguracijskih objekata, od svakog od kojih VPN zahtijeva da omogući vezu. 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.

Najčešće poruke greške na koje možete naići

Poruka

TCP5B28

Simptom

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

Stavka nije pronađena

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

PARAMETER PINBUF IS NOT VALID

Kada pokušate pokrenuti vezu, dobivate poruku koja kaže, **PARAMETER PINBUF IS NOT VALID...**

Stavka nije pronađena, Udaljeni poslužitelj ključa...

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

Nesposoban 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.

Nesposoban šifrirati ključ...

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

CPF9821

Kada pokušate proširiti ili otvoriti spremnik IP politika u iSeries^(TM) Navigatoru, pojavi se poruka CPF9821- Nije autoriziran za program QTFRPRS u QSYS knjižnici.

Drugi problemi koje možete susresti

Greška

Svi ključevi su praznine

Simptom

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

Javlja se prijava za drugi sistem

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

Ne postoji status veze

Veza nema vrijednost u stupcu **Status** u prozoru iSeries Navigatora.

Zaustavljene veze još uvijek su omogućene

Nakon što zaustavite vezu, prozor iSeries Navigatora pokazuje da je veza još uvijek omogućena.

3DES nije izbor za šifriranje

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

Prikaz neočekivanih stupaca

Postavljate stupce koje želite prikazati u prozoru iSeries Navigatora za vaše VPN veze; zatim, kada prozor kasnije pogledate, prikazuju se različiti stupci.

Neuspjeh deaktivacije aktivnih pravila filtriranja

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

Promjena grupe dinamičkih ključeva za 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.

VPN poruka greške: TCP5B28

Simptom:

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

TCP5B28: CONNECTION_DEFINITION povreda poretka

Moguće rješenje:

Pravila filtriranja koja ste pokušali aktivirati sadržavaju 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

Simptom:

Kada desno kliknete objekt u prozoru Virtualno privatno umrežavanje i izaberete ili **Svojstva** ili **Brisanje**, javlja se sljedeća poruka:



Moguće rješenje:

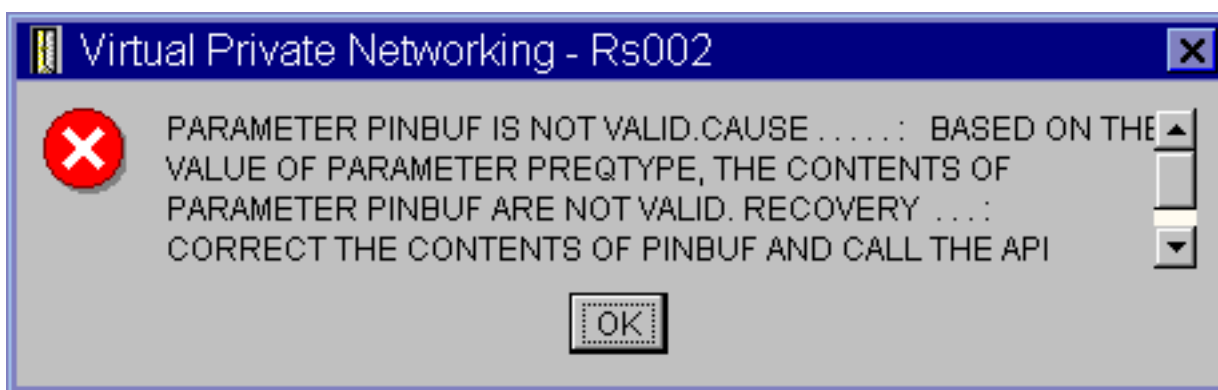
- Možda ste obrisali objekt ili ga preimenovali, a još niste osvježili prozor. Kao posljedica, objekt se još pojavljuje na prozoru Virtualno privatno umrežavanje. Da potvrdite da se radi o ovom slučaju, iz izbornika **Pogled** izaberite **Osvježi**. Ako se objekt još uvijek pojavljuje u prozoru Virtualno privatno umrežavanje, prijedite na sljedeću stavku na ovom popisu.

- Kada ste konfigurirali svojstva objekta, možda se desila komunikacijska greška između VPN poslužitelja i vaše iSeries^(TM). Mnogi od objekata koji se pojavljuju u prozoru Virtualno privatno umrežavanje 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 nastave 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 sadržava default vrijednosti). Upišite ispravne attribute objekta i izaberite **OK** da spremite vaše promjene.
- Slična greška se dešava kada pokušate obrisati objekt. Da popravite ovaj problem, ispunite list sa 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

Simptom:

Kada pokušate pokrenuti vezu, javlja se greška slična sljedećoj:



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...

Simptom:

Kada izaberete **Svojstva** za vezu dinamičkog ključa, javlja se greška slična sljedećoj:



Moguće rješenje:

Ovo se događa kada kreirate vezu sa određenim identifikatorom za udaljenog poslužitelja 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. Odavdje možete ili dodati udaljenog poslužitelja ključa natrag u grupu dinamičkog ključa, ili izabrati drugi identifikator za udaljenog poslužitelja ključa. Kliknite **OK** na listu za svojstva da spremite vaše promjene.

VPN poruka greške: Ne može se ažurirati objekt

Simptom:

Kada izaberete **OK** na listu sa svojstvima za grupu dinamičkog ključa ili ručnu vezu, javlja se sljedeća poruka:



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: Ne može se šifrirati ključ...

Simptom:

Javlja se sljedeća poruka greške:



Moguće rješenje:

QRETSVRSEC je sistemski 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 pored njega upišite 2 (promjena). Na sljedećem panelu upišite 1 i pritisnite **Enter**.

VPN poruka greške: CPF9821

Simptom:

Kada pokušate proširiti ili otvoriti spremnik IP politika u iSeries^(TM) Navigatoru, pojavi se poruka CPF9821- Nije autoriziran za program QTFRPRS u QSYS knjižnici.

Moguće rješenje:

Moguće da nemate zahtijevano ovlaštenje za dohvat trenutnog statusa Paketnih pravila ili Upravitelja VPN veze. Osigurajte da imate *IOSYSCFG ovlasti za pribavljanje pristupa na funkciju Pravila paketa u iSeries Navigatoru.

VPN greška: Svi ključevi su praznine

Simptom:

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

Moguće rješenje:

Ovo se događa svaki put kad je sistemsko vrijednost QRETSVRSEC postavljena natrag na 0. Postavljanje ove sistemsko 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. Uputite se na Poruka greške: Nesposoban šifrirati ključeve za više informacija o tome kako to napraviti.

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

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 dozvoljava iSeries^(TM) Access-u da pribavi potrebne tablice konverzije za unicode. Ovo će se desiti samo jednom.

VPN greška: Prazna vrijednost statusa u prozoru iSeries Navigatora

Simptom:

Veza nema vrijednost u stupcu **Status** u prozoru iSeries^(TM) Navigatora.

Moguće rješenje:

Prazna vrijednost statusa označava da je veza usred pokretanja. To znači, još nije u izvodenju, 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

Simptom:

Nakon što zaustavite vezu, prozor iSeries^(TM) Navigatora pokazuje da je veza još uvijek omogućena.

Moguće rješenje:

Ovo se tipično događa zato što još niste osvježili prozor iSeries Navigatora. Takav neosvježen prozor sadržava zastarjele informacije. Da ovo popravite, iz izbornika **Pogled** izaberite **Osvježi**.

VPN greška: 3DES nije izbor za šifriranje

Simptom:

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

Moguće rješenje:

Najvjerojatnije imate produkt Dobavljač kriptografičkog pristupa AC2 (5722-AC2) instaliran na vašem sistemu, a ne Dobavljač kriptografičkog pristupa AC3 (5722-AC3). AC2 dozvoljava samo algoritam za šifriranje Standard šifriranja podataka (DES) zbog ograničenja na dužinu ključa.

VPN greška: Neočekivani prikaz stupaca u prozoru iSeries Navigatora

Simptom:

Postavljate stupce koje želite prikazati u prozoru iSeries Navigatora za vaše VPN veze; zatim, kada prozor kasnije pogledate, prikazuju se različiti 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

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

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 samo 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 te 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 sa QIPFILTER dnevnikom

QIPFILTER dnevnik je lociran u knjižnici QUSRSYS i sadržava informacije o skupovima pravila filtriranja, kao i informacije o tome da li je IP datagram bio dozvoljen ili odbijen. Zapisivanje je izvedeno na osnovu opcije za vođenja dnevnika koju ste specificirali u vašim pravilima filtriranja.

Kako omogućiti dnevnik IP paketnih filtera

Koristite editor Paketnih pravila u iSeries^(TM) Navigatoru za aktivaciju QIPFILTER dnevnika. Morate omogućiti funkciju zapisivanja za svako individualno pravilo filtera. Ne postoji funkcija koja dozvoljava zapisivanje za sve IP datagrame koji ulaze ili izlaze iz sistema.

Opaska: Da omogućite QIPFILTER dnevnik, vaši filteri moraju biti deaktivirani.

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

1. U iSeries Navigatoru proširite —>**Mreža** —>**IP politike** vašeg poslužitelja.
2. Desno kliknite na **Paketna pravila** i izaberite **Konfiguracija**. Ovo prikazuje sučelje Paketna pravila.
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 datagram podudara s definicijama pravila filtriranja, radi se unos u QIPFILTER dnevnik.

Kako koristiti QIPFILTER dnevnik

OS/400^(R) automatski kreira dnevnik po prvi puta kada 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)) ENTTP((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.

Opaska: Dnevnik QIPFILTER sadržava samo dozvoljene ili odbijene unose za pravila filtriranja gdje je opcija vođenja dnevnika postavljena na FULL. Na primjer ako podesite samo PERMIT filter pravilo, IP datagramima kojima to nije izričito dozvoljeno su odbijeni. Za ove odbijene datagrame 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 datagrame 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.

Pogledajte Polja QIPFILTER dnevnika za tablicu koja opisuje QIPFILTER izlaznu datoteku.

Polja QIPFILTER dnevnika

Sljedeća tablica 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 vremenska oznaka	
TFJOB	10	N	Ime posla	
TFUSER	10	N	Profil korisnika	
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	

Ime polja	Dužina polja	Numerički	Opis	Komentari
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*

Rješavanje problema VPN-a s QVPN dnevnikom

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 nositi ovog dnevnika koristiti svakodnevno. Umjesto toga, možete ih naći korisnima za uklanjanje pogrešaka 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.

Kako omogućiti VPN dnevnik

Koristite sučelje virtualnog privatnog umrežavanja u iSeries^(TM) Navigatoru za aktiviranje 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 iSeries Navigatoru proširite → **Mreža** → **IP politike** → **Virtualno privatno umrežavanje** → **Sigurne veze** vašeg poslužitelja.
2. Za grupe dinamičkog ključa, proširite **Po grupi** i zatim desno kliknite grupu dinamičkog ključa za koju želite omogućiti vođenje dnevnika i izaberite **Svojtva**.
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:
Ništa
Ne radi se vođenje dnevnika za ovu grupu veze.

Sve

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.

Opaska: Prije nego možete zaustaviti vođenje dnevnika, provjerite da veza nije aktivna. Da promijenite status vođenja dnevnika za grupu veze, uvjerite se da nema aktivnih veza koje su pridružene toj određenoj grupi.

Kako koristiti VPN dnevnik

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)) ENTYP((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/QATOVSOFF, u korisničkoj knjižnici. Ovo možete napraviti korištenjem naredbe Kreiranje duplikata objekta (CRTDUPOBJ). Slijedi primjer naredbe CRTDUPOBJ:
CRTDUPOBJ OBJ(QATOVSOFF) 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.

Pogledajte Polja QVPN dnevnika za tablicu koja opisuje polja u QVPN izlaznoj datoteci.

Polja QVPN dnevnika

Sljedeća tablica 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	Vremenska oznaka SAA unosa	
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	

Ime polja	Dužina polja	Numerički	Opis	Komentari
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 prijenaosa	
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	
TSRFTI	6	N	Vrijeme sljedećeg osvježavanja	
TSRFLS	8	N	Vijek života osvježanja	
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	

Rješavanje problema VPN-a s dnevnicima poslova

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

Važno je da analizirate dnevnik poslova na obje strane veze ako su obje strane iSeries^(TM) poslužitelji. Kada ne uspije pokretanje dinamičke veze, od velike je pomoći ako razumijete što se događa na udaljenom sistemu.

VPN poslovi, QTOVMAN i QTOKVPNIKE, u izvodenju su na podsistemu QSYSWRK. Možete vidjeti njihove dnevnik poslova iz OS/400^(R) iSeries Navigatora.

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. Srodni dnevnik posla sadržava poruke za svaki pokušaj povezivanja koji ne uspije.

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 sa postavkom L2TP tunela, potražite poruke u ovom dnevniku posla.

Uobičajene poruke o greški VPN Upravitelja veze

Ovaj odlomak opisuje neke od najčešćih poruka o greški VPN Upravitelja veze s kojima se možete susresti.

Općenito, kada se desi greška sa VPN vezom, VPN Upravitelj veze zapisuje dvije poruke u dnevnik posla QTOVMAN. Prva poruka daje detalje koji se odnose na grešku. Možete vidjeti informacije o ovim greškama u iSeries^(TM) Navigatoru tako da kliknete desnom tipkom miša na vezu s greškom te izaberete **Informacije o greški**.

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 u greškama VPN Upravitelja veze

Poruka	Uzrok	Obnavljanje
TCP8601 Nemogućnost pokretanja VPN veze [ime veze]	Nemogućnost pokretanja ove VPN veze iz jedne od sljedećih šifri razloga: 0 - Prethodna poruka u dnevniku posla s istim imenom VPN veze ima detaljnije informacije. 1 - Konfiguracija VPN politike. 2 - Neuspjeh komunikacijske mreže. 3 - VPN Upravitelj ključa nije uspio dogovoriti novo sigurnosno udruženje. 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. Koristite iSeries Navigator da pogledate status veze. Veze koje nisu mogle biti pokrenute biti će u statusu greške.

Poruka

TCP8602

Greška se desila kod zaustavljanja VPN veze [*ime veze*]

Uzrok

Zahtijevano je zaustavljanje navedene VPN veze, međutim, veza nije zaustavljena, ili je zaustavljena uz grešku sa šifrom razloga:

- 0 - Prethodna poruka u dnevniku posla s istim imenom VPN veze ima detaljnije informacije.
- 1 - VPN veza ne postoji.
- 2 - Neuspjeh interne komunikacije sa VPN Upraviteljem ključa.
- 3 - Neuspjeh interne komunikacije s IPSec komponentom.
- 4 - Neuspjeh komunikacije s udaljenom krajnjom točkom VPN veze.

Obnavljanje

1. Provjerite dnevnik poslova za dodatne poruke.
2. Ispravite greške i pokušajte zahtjev ponovno.
3. Koristite iSeries Navigator da pogledate status veze. Veze koje nisu mogle biti pokrenute biti će u statusu greške.

TCP8604

Neuspjeh pokretanja VPN veze [*ime veze*]

Nemogućnost pokretanja ove VPN veze iz jedne od sljedećih šifri razloga:

- 1 - Nemogućnost prevođenja imena udaljenog hosta u 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 iz grupe veze.
- 9 - Tip identifikatora nije važeći.

1. Provjerite dnevnik poslova za dodatne poruke.
2. Ispravite greške i pokušajte zahtjev ponovno.
3. Koristite iSeries Navigator za provjeru ili ispravak konfiguracije VPN politike. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti.

TCP8605

VPN Upravitelj veze nije u mogućnosti komunicirati s VPN Upraviteljem ključa.

VPN Upravitelj veze zahtijeva usluge od VPN Upravitelja ključa za uspostavu sigurnosnih udruženja za dinamičke VPN veze. VPN Upravitelj veze nije u mogućnosti komunicirati s VPN Upraviteljem ključa.

1. Provjerite dnevnik 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).
Opaska: Ovo uzrokuje završetak svih trenutnih VPN veza.

Poruka

TCP8606

VPN Upravitelj ključa nije mogao uspostaviti sigurnosno udruženje zahtijevano za vezu [*ime veze*]

Uzrok

VPN Upravitelj ključa nije mogao uspostaviti zahtijevano sigurnosno udruženje iz jedne od sljedećih šifri razloga:
24 - Nije uspjela provjera autentičnosti veze ključem 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.

Obnavljanje

1. Provjerite dnevnik poslova za dodatne poruke.
2. Ispravite greške i pokušajte zahtjev ponovno.
3. Koristite iSeries Navigator za provjeru ili ispravak konfiguracije VPN politike. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti.

TCP8608

VPN veza [*ime veze*] nije mogla dobiti NAT adresu

Ova grupa dinamičkog ključa ili veza podataka specificirala je da prijevod mrežne adrese (NAT) bude učinjen na jednoj ili više adresa i da nije uspio, najvjerojatnije zbog jedne od ovih šifri razloga:
1 - Adresa na koju se treba primijeniti NAT nije jednostruka IP adresa.
2 - Sve dostupne adrese su već korištene.

1. Provjerite dnevnik poslova za dodatne poruke.
2. Ispravite greške i pokušajte zahtjev ponovno.
3. Koristite iSeries Navigator da provjerite ili ispravite VPN politiku. Osigurajte da grupa dinamičkog ključa pridružena ovoj vezi ima konfigurirane prihvatljive vrijednosti za adrese.

TCP8620

Lokalna krajnja točka veze nije dostupna

Nije moguće omogućiti ove VPN veze jer lokalna krajnja točka veze nije dostupna.

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Osigurajte da je lokalna krajnja točka veze definirana i pokrenuta korištenjem naredbe NETSTAT OPTION(*IFC).
3. Ispravite moguće greške i pokušajte zahtjev ponovno.

TCP8621

Lokalna krajnja točka za podatke nije dostupna

Nije moguće omogućiti ove VPN veze jer lokalna krajnja točka za podatke nije dostupna.

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Osigurajte da je lokalna krajnja točka veze definirana i pokrenuta korištenjem naredbe NETSTAT OPTION(*IFC).
3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Poruka	Uzrok	Obnavljanje
TCP8622 Sažimanje prijenosa nije dozvoljeno pomoću prilaza	Nije moguće omogućiti ove VPN veze, jer je navedena politika navela način sažimanja prijenosa, a ova je veza definirana kao sigurnosni prilaz.	<ol style="list-style-type: none"> 1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu. 2. Koristite iSeries Navigator da promijenite VPN politiku pridruženu ovoj VPN vezi. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8623 Preklapanje VPN veze sa već postojećom vezom	Nije moguće omogućiti ovu VPN vezu jer je postojeća VPN veza već omogućena. Ova veza ima lokalnu krajnju točku podataka [<i>vrijednost lokalne krajnje točke podataka</i>] i udaljenu krajnju točku podataka [<i>vrijednost udaljene krajnje točke podataka</i>].	<ol style="list-style-type: none"> 1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu. 2. Koristite iSeries Navigator da pogledate sve omogućene veze koje imaju lokalne krajnje točke podataka i udaljene krajnje točke podataka koje se preklapaju s vezom. Ako su zahtijevane obje veze, promijenite politiku postojeće veze. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.
TCP8624 VPN veza nije unutar djelokruga pridruženog pravila filtriranja politike	Nije moguće omogućiti VPN vezu jer krajnje točke podataka nisu unutar definiranog pravila filtriranja politike.	<ol style="list-style-type: none"> 1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu. 2. Koristite iSeries Navigator za prikaz ograničenja za krajnju točku podataka za ovu vezu ili grupu dinamičkog ključa. 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.
TCP8625 VPN veza nije prošla provjeru ESP algoritma	Nije moguće omogućiti ovu VPN vezu jer tajni ključ pridruženi vezi nije bio dovoljan.	<ol style="list-style-type: none"> 1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu. 2. Koristite iSeries Navigator za prikaz politike pridružene ovoj vezi i upišite različiti tajni ključ. 3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Poruka

TCP8626

Krajnja točka VPN veze nije ista kao krajnja točka podataka

Uzrok

Ova VPN veza nije bila moguća, jer politika navodi da je host i da krajnja točka VPN veze nije ista kao krajnja točka podataka.

Obnavljanje

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Koristite iSeries Navigator za prikaz ograničenja za krajnju točku podataka za ovu vezu ili grupu dinamičkog ključa. 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 filtriranja politike

Pravilo filtriranja politike za ovu vezu nije aktivno.

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Koristite iSeries Navigator za prikaz aktivnih filtera za politiku. Provjerite pravilo filtriranja politike za ovu vezu.
3. Ispravite moguće greške i pokušajte zahtjev ponovno.

TCP8629

Ispušten je IP paket za VPN vezu

Ova VPN veza ima konfiguriran VPN NAT i zahtijevani skup NAT adresa je premašio dostupne NAT adrese.

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Koristite iSeries Navigator da povećate broj NAT adresa dodijeljenih ovoj VPN vezi.
3. Ispravite moguće greške i pokušajte zahtjev ponovno.

TCP862A

Neuspjeh pokretanja PPP veze

Ova VPN veza je pridružena PPP profilu. Kada je pokrenuta, učinjen je pokušaj za pokretanje PPP profila, ali došlo je do neuspjeha.

1. Provjerite dnevnik poslova za dodatne poruke koje se odnose na ovu vezu.
2. Provjerite dnevnik posla pridružen PPP vezi.
3. Ispravite moguće greške i pokušajte zahtjev ponovno.

Rješavanje problema VPN-a praćenjem OS/400 komunikacija

iSeries^(TM) OS/400^(R) pruža mogućnost praćenja podataka kroz komunikacijsku liniju, kao što je sučelje mreže lokalnog područja (LAN) ili mreže širokog područja (WAN). Prosječni korisnik možda neće shvatiti cijeli sadržaj podataka praćenja. Ipak, 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 (Objekt konfiguracije)

Ime objekta konfiguracije koji se prati. Objekt je ili opis linije, opis mrežnog sučelja, ili opis mrežnog poslužitelja.

CFGTYPE(Tip konfiguracije)

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

MAXSTG (Veličina međuspremnik)

Veličina međuspremnik za praćenje. Default vrijednost je postavljena na 128 KB. Raspon ide od 128 KB do 64 MB. Stvarna maksimalna veličina međuspremnik širom sistema definirana je u sklopu Alata sistemskih usluga (SST). Stoga, možete primiti poruku greške kada koristite veću veličinu međuspremnik za naredbu STRCMNTRC nego što je definirano u SST-u. Imajte na umu da zbroj veličina međuspremnik specificiranih na svih pokrenutih praćenjima komunikacija ne smije premašiti maksimalnu veličinu međuspremnik 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 (Praćenje puno)

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 zapisi praćenja prepisuju se novima onim redoslijedom kojim se sakupljaju.

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

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 (Objekt konfiguracije)

Ime objekta konfiguracije za koji se praćenje izvodi. Objekt je ili opis linije, opis mrežnog sučelja, ili opis mrežnog poslužitelja.

CFGTYPE(Tip konfiguracije)

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. Nastojte spool datoteku držati što je moguće manjom. To analizu čini bržom i djelotvornijom. U slučaju VPN problema, filtrirajte samo IP promet te 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 (Objekt konfiguracije)

Ime objekta konfiguracije za koji se praćenje izvodi. Objekt je ili opis linije, opis mrežnog sučelja, ili opis mrežnog poslužitelja.

CFGTYPE(Tip konfiguracije)

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

FMTTCP (Formatiranje TCP/IP podataka)

Da li formatirati praćenje za TCP/IP i UDP/IP podatke. Specificirajte *YES za formatiranje praćenja za IP podatke.

TCPIPADR (Formatiranje 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 (Broj IP porta)

Broj IP porta za filtriranje.

FMTBCD (Formatiranje emitiranih podataka)

Da li su svi emitirani okviri ispisani. 'Da' je default. Ako ne želite, na primjer, zahtjeve Protokola za rezolucije adrese (ARP), navedite *NO; u suprotnom možete biti zatrpani emitiranim porukama.

Srodne informacije za VPN

Za više scenarija i opisa za VPN konfiguracije, pogledajte ove ostale izvore informacija:

- **OS/400^(R) V5R1 Virtualne privatne mreže: Udaljeni pristup na IBM^(R) e(log) poslužitelj iSeries^(TM) Poslužitelj s Windows^(R) 2000 VPN Klijentima, REDP0153**



Ovaj IBM Redpaper pruža proces konfiguriranja VPN tunela korak po korak koristeći V5R1 VPN i Windows 2000 integriranu L2TP i IPsec podršku.

- **AS/400^(R) Internet sigurnost: Implementiranje AS/400 Virtualnih privatnih mreža, SG24-5404-00**



Ovaj redbook istražuje VPN koncepte i opisuje njihovu primjenu korištenjem IP sigurnosti (IPsec) i Sloj 2 Tunelskog protokola (L2TP) na OS/400.

- **Scenariji Internet Sigurnosti za AS/400: Praktični pristup, SG24-5954-00**



Ovaj redbook istražuje sve integrirane sigurnosne mogućnosti dostupne na OS/400 sistemu kao što su IP filteri, NAT, VPN, HTTP proxy poslužitelj, SSL, DNS, primopredaja pošte, revidiranje i zapisivanje. On opisuje njihovu upotrebu kroz praktične primjere.

- **Virtualno Privatno Umrežavanje: Osiguravanje veza**



Ova Web stranica osvjetljava najnovije VPN vijesti, ispisuje zadnje PTF-ove, povezuje druge zanimljive stranice.

- **Ostali priručnici i redbook-ovi vezani uz sigurnost**

Otiđite ovdje za popis informacija vezanih uz sigurnost, a dostupnih online.

Da spremite PDF na vašu radnu stanicu za kasnije gledanje i ispis:

1. Desno kliknite PDF u vašem pretražitelju (desno kliknite na vezu iznad).
2. Kliknite **Spremi cilj kao...**
3. Otiđite do direktorija u koji želite spremiti PDF.
4. Kliknite **Spremi**.

Ako vam je potreban Adobe Acrobat Reader da pogledate ili ispišete ove PDF-ove, možete ga učitati sa Adobe Web stranice (www.adobe.com/prodindex/acrobat/readstep.html)



Dodatak. Napomene

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

IBM možda ne nudi proizvode, usluge ili funkcije o kojima se raspravlja u ovom dokumentu u drugim državama. Posavjetujte se s lokalnim IBM predstavnicima za informacije o proizvodima i uslugama koje su dostupne 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 koja se ne kosi s nekim IBM pravom intelektualnog vlasništva, se može koristiti u zamjenu. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM možda ima patente ili patente u toku za aplikacije koje pokrivaju teme koje su opisane u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakve licence na ove patente. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci za dvo-bajte informacije (DBCS), kontaktirajte odjel IBM Intelektualnog vlasništva u vašoj državi ili pošaljite upite, u pismenom obliku na:

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

Sljedeći paragraf se ne odnosi na Ujedinjeno Kraljevstvo ili bilo koju drugu državu gdje takav način nije konzistentan s lokalnim zakonom: INTERNATIONAL BUSINESS MACHINES CORPORATION PRUŽA OVU PUBLIKACIJU "KAKVA JE", BEZ BILO KAKVIH JAMSTAVA, BILO IZRAVNIH ILI NEIZRAVNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, NEIZRAVNA JAMSTVA O NE-NARUŠAVANJU, MOGUĆNOSTI PRODAJE ILI PRIKLADNOSTI 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. Promjene se povremeno rade u ovim informacijama; te promjene će biti uključene u nova izdanja publikacije. IBM može napraviti poboljšanja i/ili promjene proizvoda i/ili programa opisanog(ih) u ovoj publikaciji u bilo koje vrijeme bez 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 korištenje tih Web stranica je na vaš vlastiti rizik.

IBM može koristiti ili distribuirati bilo koje informacije koje pružite, 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 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licenci program opisan u ovim informacijama i sav licencni materijal koji je za to dostupan je pružen od strane IBM-a pod uvjetima IBM Korisničkog Ugovora, IBM Međunarodnog ugovora o programskim licencama ili bilo kakvog ekvivalentnog ugovora između nas.

Svi podaci o performansama koji se ovdje nalaze su određivani u kontroliranim uvjetima. Zbog toga se rezultati koji se dobiju u drugim radnim okolinama mogu znatno razlikovati. Neka mjerenja su možda rađena na sistemima na razvojnoj razini i nema jamstava da će rezultati mjerenja biti isti i na općenito dostupnim sistemima. Uz to, moguće je da su neka mjerenja procijenjena koristeći ekstrapolaciju. Stvarni rezultati se mogu razlikovati. Korisnici dokumenta bi trebali provjeriti primjenjive podatke za njihovo specifično okruženje.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi točnost performansi, kompatibilnosti ili bilo koje druge izjave koje su vezane za ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave koje se tiču IBM-ovih budućih smjernica ili namjera su podložne promjenama i povlačenju bez posebnih obavijesti i predstavljaju samo ciljeve.

Sve IBM cijene koje su ovdje prikazane su IBM-ove preporučene cijene za zastupnike, vrijede u ovom trenutku i podložne su promjeni bez posebne obavijesti. Cijene zastupnika se mogu razlikovati.

Ove informacije su samo za svrhu planiranja. Informacije ovdje navedene su podložne promjeni prije nego opisani proizvodi postanu dostupni.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnom poslu. Da bi ih se u potpunosti objasnilo, primjeri uključuju imena pojedinaca, poduzeća, marki i proizvoda. Sva ta imena su izmišljena i bilo kakva sličnost sa imenima i adresama korištenima u stvarnom poduzeću je u potpunosti slučajna.

Zaštitni znaci

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

Application System/400

AS/400

e (logo)

IBM

iSeries

Operating System/400

OS/400

400

Lotus, Freelance i WordPro su zaštitni znakovi od International Business Machines Corporation i Lotus Development Corporation u Sjedinjenim Državama, drugim državama ili oboje.

C-bus je zaštitni znak Corollary, Inc. u Sjedinjenim Državama, drugim državama ili oboje.

ActionMedia, LANDesk, MMX, Pentium i ProShare su zaštitni znakovi ili registrirani zaštitni znakovi Intel Corporation u Sjedinjenim Državama, drugim državama ili oboje.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znakovi od Microsoft Corporation u Sjedinjenim Državama, drugim državama ili oboje.

SET i SET Logo su zaštitni znakovi čiji je vlasnik SET Secure Electronic Transaction LLC.

Java i svi Java-zasnovani zaštitni znakovi su zaštitni znakovi od Sun Microsystems, Inc. u Sjedinjenim Državama, drugim državama ili oboje.

UNIX je registrirani zaštitni znak od The Open Group u Sjedinjenim Državama i drugim državama.

Druga imena poduzeća, proizvoda i usluga mogu biti zaštitni znaci ili trgovački znaci od drugih.

Termini i uvjeti za spuštanje i ispis publikacija

Dozvole za upotrebu publikacija koje ste izabrali za spuštanje su podložne sljedećim terminima i uvjetima i vašem prihvaćanju istih.

Osobna upotreba: Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz osiguranje da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili koristiti za izradu drugih radova ove Publikacije ili bilo koji njihov dio, bez izričitog pristanka IBM-a.

Komercijalna upotreba: Možete reproducirati, distribuirati i prikazivati ove publikacije isključivo unutar vašeg poduzeća, uz osiguranje da su sve napomene o vlasništvu sačuvane. Ne smijete umnažati, distribuirati, prikazivati ili koristiti za izradu drugih radova ove Publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričitog pristanka IBM-a.

Osim ako je izričito dodijeljeno u ovoj dozvoli, nikakve druge dozvole, licence ili prava nisu dodijeljena, niti izravno niti posredno, na publikacije ili bilo koje informacije, podatke, softver ili drugo intelektualno vlasništvo sadržano unutar.

IBM zadržava pravo povlačenja dozvola ovdje danih, kad god, prema vlastitom nahođenju, ustanovi da je upotreba Publikacija u suprotnosti sa njegovim interesima ili, ukoliko utvrdi, da se gornje upute nisu ispravno slijedile.

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 O SADRŽAJU OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU "TAKVE-KAKVE-JESU" I BEZ IKAKVIH JAMSTAVA BILO KAKVE VRSTE, BILO IZREČENIH ILI INDIKATIVNIH, UKLJUČUJUĆI, ALI NE I OGRANIČAVAJUĆI SE NA, INDIKATIVNA JAMSTVA O PRODAJNOJ VRIJEDNOSTI I PRIKLADNOSTI ZA ODREĐENU SVRHU.

Na sav materijal IBM Corporation polaže autorsko pravo.

Spuštanjem i ispisom publikacija s ove stranice, naznačili ste da se slažete s ovim terminima i uvjetima.



Tiskano u Hrvatskoj