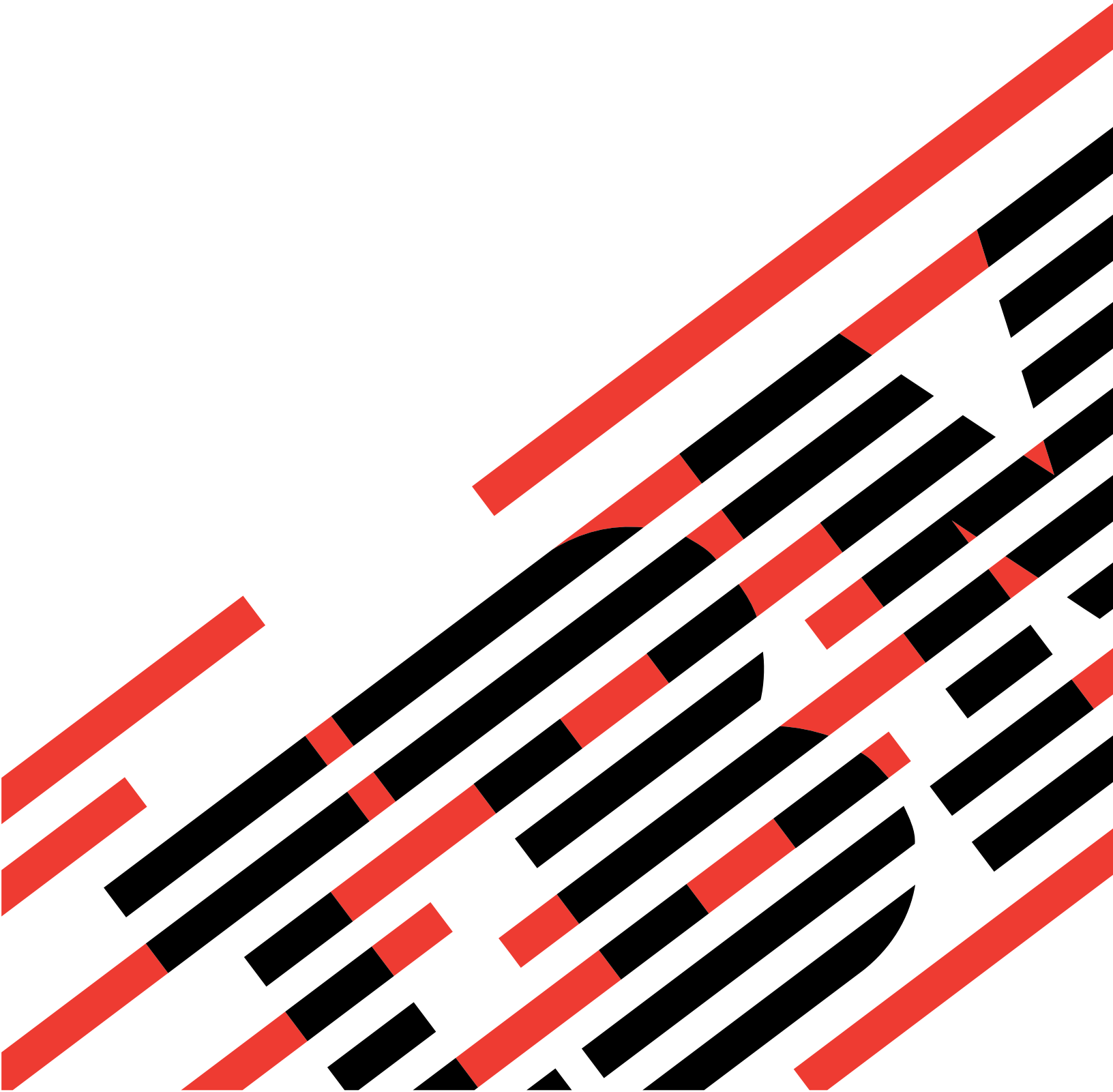
IBM

eserver

iSeries

Delo z navideznim zasebnim omrežjem

Različica 5 izdaja 3



IBM

@server

iSeries

Delo z navideznim zasebnim omrežjem

Različica 5 izdaja 3

Opomba

Preden začnete uporabljati te informacije in izdelek, kateremu so namenjene, preglejte “Opombe”, na strani 65.

Šesta izdaja (avgust 2005)

Ta izdaja se nanaša na IBM i5/OS (5722-SS1) različice 5, izdaje 3 in ravni popravkov 2 ter na vse naslednje izdaje in ravni popravkov, dokler v novih izdajah ne bo navedeno drugače. Ta različica se ne izvaja na vseh modelih RISC (računalnik z zoženim naborom ukazov), niti na modelih CISC.

Kazalo

Delo z navideznim zasebnim omre┼żjem 1

Kaj je novega v V5R3 2
Natisni to temo 3
Scenariji VPN 3
Scenarij VPN: Osnovna povezava s podru┼żnico . . . 4
Podrobnosti konfiguriranja 6
Scenarij VPN: Osnovna povezava od podjetja do podjetja 8
Podrobnosti konfiguriranja 10
Scenarij VPN: Za┼í─Żita prostovoljnega tunela L2TP z IPSec 13
Podrobnosti konfiguriranja 14
Scenarij VPN: uporaba prevoda omre┼żnega naslova za VPN 19
Koncepti VPN 20
Protokoli IPSec (IP Security) 21
Protokol Authentication Header 22
Protokol ESP (Encapsulating Security Payload) . . 23
Zdru┼żena AH in ESP 24
Upravljanje klju─Żev 24
L2TP (Layer 2 Tunnel Protocol) 25
Prevod omre┼żnega naslova za VPN 26
IPSec, zdru┼żljiv z NAT 27
Stiskanje IP (IPComp) 28
VPN in filtriranje IP 28
Selitev filtrov na─Żel v trenutno izdajo 29
Povezave VPN brez filtrov na─Żel 30
Implicitni IKE 30
Na─Żrtovanje za VPN 30
Zahteve za nastavitev VPN 30
Dolo─Żitev, katero vrsto VPN izdelati 31
Izpolnitev na─Żrtovalnih preglednic VPN 32
Na─Żrtovalna preglednica za dinami─Żne povezave 32
Na─Żrtovalna preglednica za ro─Żne povezave . . 33
Konfiguriranje VPN 35
Konfiguriranje povezav VPN s pomo─Żjo ─Żarovnika Nova povezava 36
Konfiguriranje na─Żel za za┼í─Żito VPN 37
Konfiguriranje na─Żela IKE (Internet Key Exchange) 37
Konfiguriranje podatkovnega na─Żela 37
Konfiguriranje za┼í─Żitene povezave VPN 38
Konfiguriranje ro─Żne povezave 39
Konfiguriranje pravil paketov VPN 39
Konfiguriranje pravil za filtriranje pred IPSec . . 40
Konfiguriranje pravil za filtriranje na─Żel 40
Definiranje vmesnika za pravila filtriranja VPN . . 41
Aktiviranje pravil paketov VPN 42
Zagon povezave VPN 42
Upravljanje VPN 43
Nastavitev privzetih atributov za povezave 43
Vnovi─Żna nastavitev povezav v stanju napake . . . 43
Prikaz informacij o napaki 43
Prikaz atributov aktivne povezave 44
Uporaba sledenja stre┼żnika VPN 44
Prikaz dnevnikov opravil stre┼żnika VPN 45
Prikaz atributov dogovorov za za┼í─Żito (SA) . . . 45
Zaustavitev povezave VPN 45
Brisanje konfiguracijskih objektov VPN 45
Odpravljanje te┼żav v VPN 45
Za─Żetek odpravljanja te┼żav v VPN 46
Splo┼íne konfiguracijske napake VPN in kako jih odpraviti 47
Sporo─Żilo o napaki VPN: TCP5B28 48
Sporo─Żilo o napaki VPN: postavka ni bila najdena 48
Sporo─Żilo o napaki VPN: PARAMETER PINBUF NI VELJAVEN 49
Sporo─Żilo o napaki VPN: postavka ni bila najdena, oddaljen stre┼żnik klju─Żev... 49
Sporo─Żilo o napaki VPN: objekta ni mogo─Że a┼żurirati 49
Sporo─Żilo o napaki VPN: klju─Ża ni mogo─Że ┼íifrirati... 50
Sporo─Żilo o napaki VPN: CPF9821 50
Napaka VPN: Vsi klju─Źi so prazni 50
Napaka VPN: pri uporabi pravil paketov se prika┼że prijava za drug sistem 51
Napaka VPN: prazen status povezave v oknu Navigatorja iSeries 51
Napaka VPN: povezava ima po zaustavitvi status omogo─Żena 51
Napaka VPN: 3DES ni na voljo za ┼íifriranje. . . 51
Napaka VPN: v oknu Navigatorja iSeries so prikazani nepri─Żakovani stolpci 51
Napaka VPN: Aktivnih pravil za filtriranje ni mogo─Że deaktivirati 51
Napaka VPN: skupina povezav s klju─Źi za povezavo se spremeni 52
Odpravljanje te┼żav v VPN z dnevnikom QIPFILTER 52
Polja dnevnika QIPFILTER 53
Odpravljanje te┼żav v VPN z dnevnikom QVPN . . 54
Polja dnevnika QVPN 55
Odpravljanje te┼żav v VPN z dnevniki opravil VPN . 56
Splo┼ína sporo─Żila o napakah Upravljalnika povezav VPN 57
Odpravljanje te┼żav v VPN s komunikacijskim sledenjem OS/400 61
Povezane informacije za VPN 63

Dodatek. Opombe 65

Blagovne znamke 66
Dolo─Żbe in pogoji za snemanje publikacij z oddaljenega ra─Żunalnika in njihov natis 67

Delo z navideznim zasebnim omre┼żjem

Navidezno zasebno omre┼żje (VPN) omogo─Ża, da podjetje varno raz┼íiri svoj zasebni intranet prek obstoje─Źega javnega omre┼żja kot je internet. S pomo─Źjo VPN lahko podjetje krmili omre┼żni promet, pri ─Źemer nudi pomembne funkcije za┼í─Źite kot sta overjanje in zasebnost podatkov.

OS/400(R) VPN je izbirno namestljiva komponenta Navigatorja iSeries(TM) , grafi─Źnega uporabni┼íkega vmesnika (GUI) za OS/400. Omogo─Ża izdelavo varne poti v katerikoli kombinaciji gostitelja in prehoda. OS/400 VPN zagotavlja varnost podatkov, poslanih med dvema zaklju─Źnima to─Źkama povezave, s pomo─Źjo na─Źinov overjanja, algoritmov ┼íifriranja in drugih varnostnih ukrepov.

VPN se izvaja v omre┼żni plasti skladovnega modela komunikacij TCP/IP. VPN uporablja ogrodje IPSec (IP Security Architecture). IPSec nudi osnovne funkcije za┼í─Źite za internet, in tudi pro┼żne gradnike, iz katerih lahko izdelate robustna, varna navidezna zasebna omre┼żja.

VPN podpira tudi re┼íitve VPN L2TP (Layer 2 Tunnel Protocol). Povezave L2TP, imenovane tudi navidezne linije, omogo─Żajo stro┼íkovno ustrezen dostop za oddaljene uporabnike, saj omogo─Żajo, da zdru┼żen omre┼żni stre┼żnik upravlja naslove IP, dodeljene njegovim oddaljenim uporabnikom. Povezave L2TP poleg tega nudijo tudi varen dostop do sistema ali omre┼żja, ─Źe jih za┼í─Źitite z IPSec.

Pomembno je, da razumete vpliv, ki ga bo imel VPN na celotno omre┼żje. Pravilno na─Źrtovanje in izvedba sta bistvenega pomena. Preberite naslednje teme, da boste zagotovo vedeli, kako delujejo VPN-ji in kako jih lahko uporabite:

Novosti v V5R3
Tema opisuje, katere informacije so nove ali bistveno spremenjene v tej izdaji.

Natisni to temo
─Źe si ┼żelite ogledati natisnjeno kopijo teh informacij, pojdite sem, da boste natisnili PDF.

Scenariji VPN
Preglejte te scenarije, da boste spoznali osnovne tipe VPN in korake, vklju─Żene v njihovo konfiguriranje.

Koncepti VPN
Pomembno je, da imate vsaj osnovno znanje iz standardnih tehnologij VPN. V tej temi boste na┼íli konceptne informacije o protokolih, ki jih uporablja VPN v svoji izvedbi.

Na─Źrtovanje VPN
Prvi korak za uspe┼íno uporabo VPN je na─Źrtovanje. V tej temi boste na┼íli informacije o selitvi iz prej┼ínjih izdaj, zahteve za namestitev in povezave s svetovalcem za na─Źrtovanje, ki bo ustvaril na─Źrtovalno preglednico, prilagojeno va┼íim specifikacijam.

Konfiguriranje VPN
Ko izdelate na─Źrt za VPN, lahko za─Źnete s konfiguriranjem. V tej temi boste na┼íli pregled stvari, ki jih lahko naredite z VPN in kako jih naredite.

Upravljanje VPN
Tema opisuje razli─Źne naloge, ki jih lahko izvedete za upravljanje aktivnih povezav VPN, vklju─Żno s spremembami ali brisanji, ki jih lahko opravite v nadzorniku.

Odpravljanje te┼żav v VPN
To temo preberite, ─Źe imate te┼żave v povezavah VPN.

Povezane informacije za VPN
Sem pojdite, –Że ┼żelite najti povezave na druge vire informacij VPN in s tem povezane teme.

Kaj je novega v V5R3

Izbolj┼íave funkcij
Izbolj┼íave v funkcijah za delo z navideznim zasebnim omre┼żjem (VPN) razli–Żice 5 izdaje 3 (V5R3) vklju–Żujejo dva nova tipa identifikatorjev. Pri definiranju na–Żel za izmenjavo klju–Żev VPN in zaklju–Źnih to–Źk povezovalnih podatkov lahko izberete dva nova tipa identifikatorjev. Tipa identifikatorjev sta lokalni naslov IP in ime gostitelja IPv4. Dodatne informacije najdete v zaslonski pomo–Źi Navigatorja iSeries(TM).

- **Moj lokalni naslov IP**
  Z identifikatorjem Moj lokalni naslov IP lahko v definiciji povezave definirate tip lokalnega stre┼żnika za klju–Że za na–Żelo izmenjave klju–Żev prek interneta ali lokalno zaklju–Źno to–Źko podatkov. –îe ga izberete, VPN uporablja naslov IPv4. Povezave VPN, ki uporabljajo ta tip identifikatorja, ne smejo uporabljati filtra na–Żela. Poleg tega mora biti lokalni sistem pobudnik povezave.
- **Ime gostitelja IPv4**
  Z identifikatorjem imena gostitelja IPv4 lahko definirate nekaj razli–Źnih parametrov:
  – Tip identifikatorja za oddaljeni stre┼żnik klju–Żev v na–Żelu izmenjave klju–Żev prek interneta
  – Identifikator oddaljenega naslova v lastnostih povezave
  – Definicijo filtra na–Żel za lastnosti skupine povezav

  Ime gostitelja IPv4 razre┼íi naslov IP za ime gostitelja, podanega kot tip identifikatorja.

Opomba o varnosti VPN:
Priporo–Żamo, da vedno, ko uporabite klju–Ź z vnaprej dolo–Żeno souporabo za overjanje, uporabite pogajanje glavnega na–Żina. Ta nudi bolj za┼í–Żiteno izmenjavo. –îe morate uporabiti klju–Że z vnaprej dolo–Żeno souporabo in pogajanje agresivnega na–Żina, uporabite zapletene besede, ki jih je zelo te┼żko zlomiti v napadih, ki pregledujejo slovar za gesla. Kako prisiliti izmenjavo klju–Żev, da uporabi pogajanje glavnega na–Żina, je opisano v temi Mo┼żna zloraba za┼í–Żite z overjanjem klju–Ża z vnaprej dolo–Żeno souporabo. –îe izdelate ali uredite na–Żelo izmenjave klju–Żev prek interneta, si lahko podrobnej┼íe informacije preberete tudi v zaslonski pomo–Źi Navigatorja iSeries.

Izbolj┼íave informacij
Spremembe v temi V5R3 VPN v Informacijskem centru vklju–Żujejo tudi vizualno predstavitev, ki opisuje zasnovo prostovoljnega tunela L2TP (Layer 2 Tunnel Protocol). Kliknite naslednjo povezavo, –Że ┼żelite videti vizualno predstavo o prostovoljnih tunelih L2TP, za┼í–Żitenih z IPSec. To zahteva dodatek Flash

. Ogledate si lahko tudi razli–Żico HTML te predstavitve.

Kako videti, kaj je novega ali spremenjenega

Te informacije uporabljajo za ozna–Żevanje tehni–Źnih sprememb naslednje:

- Sliko

  , ki ozna–Żuje, kje se za–Źnejo nove ali spremenjene informacije.
- Sliko

  , ki ozna–Żuje, kje se nove ali spremenjene informacije kon–Żajo.

–îe ┼żelite prebrati ┼íe druge informacije o novostih ali spremembah v tej izdaji, preberite Opomnik za uporabnike.

Natisni to temo

–îe si ┼želite ogledati ali presneti razli–Źico PDF tega dokumenta, izberite Delo z navideznim zasebnim omre┼żjem (VPN) (pribli┼żno 509 kB).

Shranitev datotek PDF

PDF shranite na delovno postajo, kjer si ga lahko ogledate ali natisnete, takole:

1. Z desno tipko mi┼íke kliknite PDF v brskalniku (z desno tipko mi┼íke kliknite zgornjo povezavo).
2. Kliknite **Shrani cilj kot...**, –Źe uporabljate Internet Explorer. –îe uporabljate Netscape Communicator, kliknite **Shrani povezavo kot...**.
3. Izberite imenik, v katerega ┼želite shraniti razli–Źico PDF.
4. Kliknite **Save**.

Snemanje programa Adobe Acrobat Reader

Za prikaz ali tiskanje teh PDF-jev potrebujete program Adobe Acrobat Reader. Kopijo lahko presnamete s spletne strani Adobe (www.adobe.com/products/acrobat/readstep.html)

.

Scenariji VPN

Preglejte naslednje scenarije, ki vas bodo seznanili s tehni–Źnimi in konfiguracijskimi podrobnostmi za naslednje osnovne tipe povezav:

- **Scenarij VPN: osnovna povezava s podru┼żnico**
  V tem scenariju ┼želi va┼íe podjetje vzpostaviti povezavo VPN med podmre┼żami dveh oddaljenih oddelkov prek para ra–Źunalnikov iSeries(TM), ki delujeta kot prehoda VPN.
- **Scenarij VPN: osnovna povezava od podjetja do podjetja**
  V tem scenariju ┼želi va┼íe podjetje vzpostaviti VPN med odjemalsko delovno postajo v proizvodnem oddelku in odjemalsko delovno postajo v dobavnem oddelku va┼íega poslovnega partnerja.
- **Scenarij VPN: za┼í–Žita prostovoljnega tunela L2TP z IPSec**
  Scenarij ka┼że povezavo med gostiteljem podru┼żnice in glavno pisarno, ki uporablja L2TP, za┼í–Žiten z IPSec. Podru┼żnica ima dinami–Źno dodeljen naslov IP, glavna pisarna pa stati–Žen naslov IP z mo┼żnostjo globalnega usmerjanja.
- **Scenarij VPN: uporaba prevoda omre┼żnega naslova za VPN**
  V tem scenariju ┼želi va┼íe podjetje izmenjati pomembne podatke s poslovnim partnerjem s pomo–Źjo VPN OS/400(R). Za nadaljnjo za┼í–Žito zasebnosti omre┼żne strukture bo va┼íe podjetje uporabilo tudi VPN NAT, s katerim bo skrilo zasebni naslov IP iSeries, ki ga uporablja za gostovanje aplikacij, do katerih ima dostop va┼í poslovni partner.

Dodatni scenariji VPN

Dodatne konfiguracijske scenarije VPN lahko najdete v naslednjih virih informacij o VPN:

- **Scenarij QoS: za┼í–Žiteni in predvidljivi rezultati (VPN in QoS)**
  Z VPN lahko izdelate tudi na–Žela kakovosti storitve (QoS). Zgled ka┼że njuno skupno rabo.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153**

  V tej IBM-ovi rde–Źi knjigi boste na┼íli postopek, ki po korakih opisuje konfiguriranje tunela VPN s pomo–Źjo VPN V5R1 in vgrajene podpore Windows 2000 za L2TP in IPSec.

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

  Rde─Źa knjiga razlaga koncepte VPN in opisuje njegovo izvedbo s pomo─Źjo IPSec (IP security) in L2TP (Layer 2 Tunneling Protocol) v OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  Rde─Źa knjiga razlaga vse vgrajene funkcije omre┼żne za┼í─Źite, ki so na voljo v sistemu OS/400, kot so filtri IP, NAT, VPN, stre┼żnik proxy HTTP, SSL, DNS, podajanje po┼íte, nadzorovanje in bele┼żenje. Njihovo uporabo opi┼íe s pomo─Źjo prakti─Źnih zgledov.

Scenarij VPN: Osnovna povezava s podru┼żnico

Denimo, da ┼żeli va┼íe podjetje zmanj┼íati stro┼íke, ki jih povzro─Źa komuniciranje med podru┼żnicami. Va┼íe podjetje uporablja frame ali zakupljeno linijo, toda ┼żelite raziskati druge mo┼żnosti za prenos notranjih zaupnih podatkov, ki so cenej┼íe, varnej┼íe in globalno dostopne. Z uporabo interneta lahko preprosto vzpostavite zasebno navidezno omre┼żje (VPN), ki bo zadovoljilo potrebe va┼íega podjetja.

Va┼íe podjetje in njegove podru┼żnice zahtevajo povezavo VPN za internet, ne pa tudi znotraj njihovih intranetov. Ker menite, da so intraneti varni, je najbolj┼ía re┼íitev izdelava VPN od prehoda do prehoda. V tem primeru sta povezana oba prehoda neposredno s posredni┼íkim omre┼żjem. Z drugimi besedami povedano sta *mejna* ali *obrobna* sistema, ki nista za┼í─Źitena s po┼żarnim zidom. Zgled vam bo koristil kot uvod v korake, vklju─Ćene v nastavitev osnovne konfiguracije VPN. ─Źe je v tem scenariju omenjen izraz *internet*, se nana┼ía na posredni┼íko omre┼żje med dvema prehodoma VPN, ki sta lahko zasebno omre┼żje podjetja ali javni internet.

> **Pomembna opomba:**
> V tem scenariju sta priklju─Ćena za┼í─Źitna prehoda iSeries(TM) neposredno v internet. Po┼żarnega zidu nismo vklju─Źili zato, da bi poenostavili scenarij, kar pa ne pomeni, da uporaba po┼żarnega zidu ni potrebna. Pravzaprav razmislite o vseh tveganjih, povezanih z za┼í─Źito, vsaki─Ć ko se pove┼żete v internet. V rde─Źi knjigi AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> boste na┼íli podroben opis razli─Źnih na─Źinov za zmanj┼íanje teh tveganj.

Prednosti

Scenarij ima naslednje prednosti:
- Uporaba interneta ali obstoje─Źega intraneta zmanj┼ía stro┼íek zasebnih linij med oddaljenimi podmre┼żami.
- Uporaba interneta ali obstoje─Źega intraneta zmanj┼ía zapletenost namestitve in vzdr┼ževanja zasebnih linij in z njimi povezane opreme.
- Uporaba interneta omogo─Ća povezavo oddaljenih mest skoraj z vsemi mesti na svetu.
- Uporaba VPN nudi uporabnikom dostop do vseh stre┼żnikov in sredstev na katerikoli strani povezave kot ─Će bi bili povezani z uporabo zakupljene linije ali povezave javnega omre┼żja (WAN).
- Uporaba ┼íifriranja in na─Źinov overjanja v skladu z industrijskim standardom zagotavlja za┼í─Źito pomembnih informacij, ki potujejo z enega mesta na drugo.
- Dinami─Źna in redna izmenjava ┼íifrirnih klju─Źev poenostavlja nastavitev in zmanj┼ía tveganje, povezano z dekodiranjem klju─Źev in luknjami v za┼í─Źiti.
- Uporaba zasebnih klju─Źev IP v vsaki oddaljeni podmre┼ži onemogo─Ća dodelitev pomembnih javnih naslovov IP vsem odjemalcem.

Cilji

V tem scenariju ┼żeli Mojepodjetje vzpostaviti VPN med podmre┼żama ra─Źunovodskega in tehni─Źnega oddelka

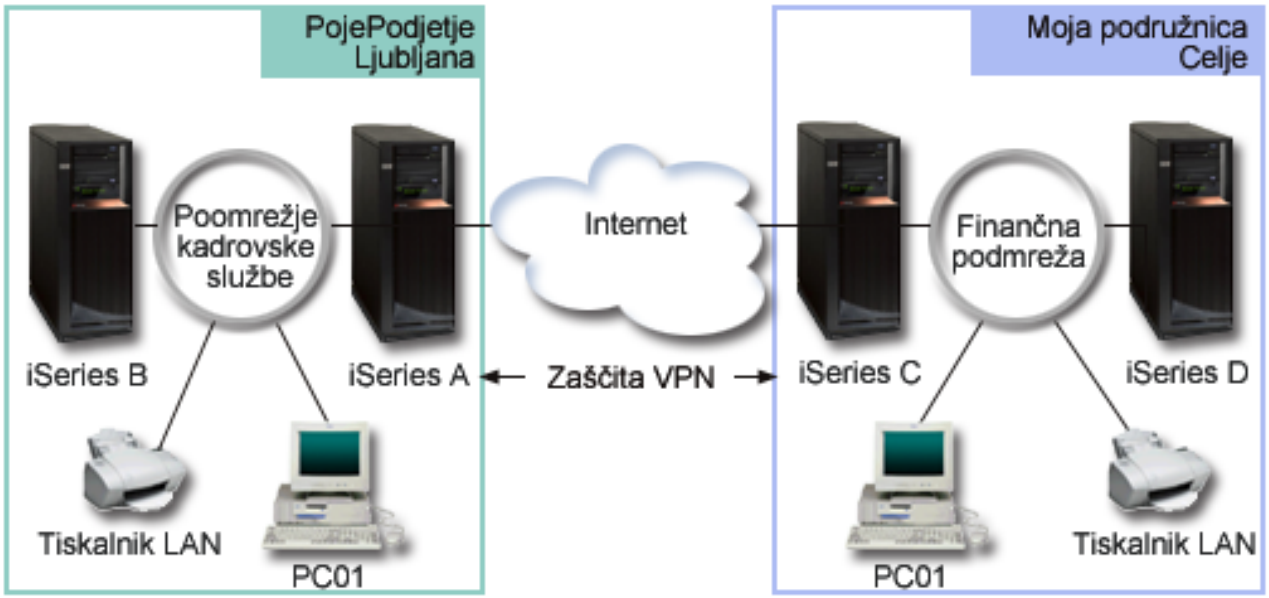
prek para stre┼żnikov iSeries. Oba stre┼żnika bosta delovala kot prehoda VPN. Po dolo─Źbah konfiguracij VPN izvaja prehod upravljanje klju─Źev in uveljavlja IPSec za podatke, ki potujejo prek tunela. Prehod ni podatkovna zaklju─Źna to─Źka povezave.

Cilji tega scenarija so naslednji:

- VPN mora ┼í─Źititi ves podatkovni promet med podmre┼żo tehni─Źnega oddelka in podmre┼żo ra─Źunovodskega oddelka.
- Promet podatkov ne zahteva ve─Ź za┼í─Źite VPN, ko dose┼że eno od podmre┼ż oddelka.
- Vsi odjemalci in gostitelji v vsaki podmre┼żi imajo popoln dostop do drugega omre┼żja, vklju─Źno z vsemi aplikacijami.
- Stre┼żnika prehoda lahko medsebojno komunicirata in dostopata do aplikacij.

Podrobnosti

Naslednja slika ka┼że omre┼żne zna─Źilnosti za Mojepodjetje.



Tehni─Źni oddelek

- V iSeries-A se izvaja OS/400(R) razli─Źice 5 izdaje 2 (V5R2) in deluje kot prehod VPN tehni─Źnega oddelka.
- Podmre┼ža je 10.6.0.0, maska pa 255.255.0.0. Ta podmre┼ža predstavlja podatkovno zaklju─Źno to─Źko tunela VPN za Mojepodjetje v Ljubljani.
- iSeries-A se pove┼že v internet z naslovom IP 204.146.18.227. To je zaklju─Źna to─Źka povezave. iSeries-A tako izvaja upravljanje klju─Źev in uveljavlja IPSec za vhodne in izhodne datagrame IP.
- iSeries-A se pove┼že s svojo podmre┼žo z naslovom IP 10.6.11.1.
- iSeries-B je proizvodni stre┼żnik tehni─Źnega oddelka, na katerem se izvajajo standardne aplikacije TCP/IP.

Ra─Źunovodski oddelek

- V iSeries-C se izvaja OS/400 razli─Źice 5 izdaje 2 (V5R2) in deluje kot prehod VPN ra─Źunovodskega oddelka.
- Podmre┼ža je 10.196.8.0, maska pa 255.255.255.0. Podmre┼ža predstavlja podatkovno zaklju─Źno to─Źko tunela VPN za Mojepodjetje v Kr┼íkem.
- iSeries-C se pove┼že v internet z naslovom IP 208.222.150.250. To je zaklju─Źna to─Źka povezave. iSeries-C tako izvaja upravljanje klju─Źev in uveljavlja IPSec za vhodne in izhodne datagrame IP.

- iSeries-C se pove┼že s svojo podmre┼žo z naslovom IP 10.196.8.5.

Konfiguracijske naloge

Za konfiguriranje povezave podru┼žnice, opisane v tem scenariju, morate opraviti vse izmed naslednjih nalog:

1. Preverite usmerjanje TCP/IP in zagotovite, da lahko stre┼żnika prehoda komunicirata prek interneta. To zagotavlja, da bodo gostitelji v vsaki podmre┼ži pravilno izvajali usmeritve v ustrezen prehod za dostop do oddaljene podmre┼že.
   Opomba: Usmerjanje je predmet, ki presega namen te teme. ─če imate vpra┼íanja, preberite temo Informacijskega centra z naslovom Usmerjanje TCP/IP in uravnote┼ženje obremenitve.
2. Izpolnite (stran 6) na─Źrtovalne preglednice in potrditvene sezname za oba sistema.
3. Konfigurirajte (stran 7) VPN za prehod VPN tehni─Źnega oddelka (iSeries-A).
4. Konfigurirajte (stran 8) VPN za prehod VPN ra─Źunovodskega oddelka (iSeries-C).
5. Preverite, ali sta stre┼żnika VPN zagnana (stran 8).
6. Preizkusite (stran 8) komunikacije med oddaljenima podmre┼žama.

Podrobnosti konfiguriranja

Ko dokon─Źate prve korake in preverite, ali usmerjanje TCP/IP pravilno deluje in stre┼żnika prehoda lahko komunicirata, lahko za─Źnete s konfiguriranjem VPN.

2. korak: Izpolnite na─Źrtovalne preglednice

Naslednji na─Źrtovalni potrditveni seznami ka┼żejo vrsto informacij, ki jih potrebujete, preden za─Źnete konfigurirati VPN. Preden za─Źnete z nastavitvijo VPN, morajo biti vsi odgovori na predpogojnem potrditvenem seznamu DA.

Opomba: Te preglednice veljajo za iSeries-A, postopek ponovite tudi za iSeries-C in po potrebi zamenjajte naslov IP.

Predpogojni potrditveni seznam	Odgovori
Ali uporabljate OS/400(R) izdaje V5R2 (5722-SS1) ali novej┼íe?	Da
Ali ste namestili Upravljalnik digitalnih potrdil (mo┼žnost 5722-SS1 34)?	Da
Ali ste namestili ponudnik ┼íifriranega dostopa (5722-AC2 ali AC3)?	Da
Ali ste namestili iSeries(TM) Access za Windows(R) (5722-XE1)?	Da
Ali ste namestili Navigator iSeries?	Da
Ali ste namestili omre┼žno podkomponento Navigatorja iSeries?	Da
Ali ste namestili pomo┼žne programe TCP/IP za povezljivost za OS/400 (5722-TC1)?	Da
Ali ste nastavili sistemsko vrednost za ohranitev za┼í─Źitnih podatkov stre┼żnika (QRETSVRSEC *SEC) na 1?	Da
Ali je na iSeries konfiguriran TCP/IP (vklju─Źno z vmesniki IP, smermi, imenom lokalnega gostitelja in imenom lokalne domene)?	Da
Ali je med zahtevanima zaklju─Źnima to─Źkama vzpostavljeno obi─Źajno komuniciranje TCP/IP?	Da
Ali ste uveljavili najnovej┼íe za─Źasne popravke programa (PTF-je)?	Da
Ali pravila za filtriranje po┼żarnega zidu ali usmerjevalnika podpirajo protokola AH in ESP, ─Će pre─Źka tunel VPN po┼żarne zidove ali usmerjevalnike, ki uporabljajo pravila za filtriranje paketov IP?	Da
Ali so po┼żarni zidovi in usmerjevalniki konfigurirani tako, da dopu┼í─Źajo protokole IKE (UDP vrata 500), AH in ESP?	Da
Ali so po┼żarni zidovi konfigurirani tako, da omogo─Źajo odpo┼íiljanje IP?	Da

Te informacije potrebujete za konfiguriranje VPN	Odgovori
Kak┼íno vrsto povezave izdelujete?	Od prehoda do prehoda
Kako boste poimenovali skupino dinami─Źnih klju─Źev?	HRgw2FINgw
Kak┼íno vrsto za┼í─Źite in zmogljivosti sistema potrebujete za za┼í─Źito klju─Źev?	Uravnote┼żeno
Ali overjate povezavo s pomo─Źjo potrdil? ─Če ne, kak┼íen je klju─Ź z vnaprej dolo─Źeno skupno rabo?	Ne visokozaupen
Kak┼íen je identifikator lokalnega stre┼żnika klju─Źev?	Naslov IP: 204.146.18.227
Kak┼íen je identifikator lokalne podatkovne zaklju─Źne to─Źke?	Podmre┼ža: 10.6.0.0 Maska: 255.255.0.0
Kak┼íen je identifikator oddaljenega stre┼żnika klju─Źev?	Naslov IP: 208.222.150.250
Kak┼íen je identifikator oddaljene podatkovne zaklju─Źne to─Źke?	Podmre┼ža: 10.196.8.0 Maska: 255.255.255.0
Katera vrata in protokole ┼żelite dovoliti za povezavo?	Katerakoli
Kak┼íno vrsto za┼í─Źite in zmogljivosti sistema potrebujete za za┼í─Źito podatkov?	Uravnote┼żeno
Na katere vmesnike se nana┼ía povezava?	TRLINE

3. korak: Konfigurirajte VPN na iSeries-A

S pomo─Źjo informacij iz preglednic konfigurirajte VPN na iSeries-A:

1. V Navigatorju iSeries raz┼íirite iSeries-A —**>Omre┼żje—>Na─Źela IP**.
2. Z desno tipko mi┼íko kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Nova povezava**, da boste zagnali ─Źarovnika Nova povezava.
3. Na **naslovni** strani si oglejte informacije o objektih, ki jih izdela ─Źarovnik.
4. Kliknite **Naprej**, da boste odprli stran **Ime povezave**.
5. V polje **Ime** vnesite HRgw2FINgw.
6. (izbirno) Podajte opis te povezovalne skupine.
7. Kliknite **Naprej**, da boste odprli stran **Scenarij povezave**.
8. Izberite **Pove┼żi prehod z drugim prehodom**.
9. Kliknite **Naprej**, da boste odprli stran **Na─Źelo izmenjave internetnih klju─Źev**.
10. Izberite **Izdelaj novo na─Źelo**, nato pa izberite **Uravnote┼żi za┼í─Źito in zmogljivost**.
11. Kliknite **Naprej**, da boste odprli stran **Potrdilo za lokalno zaklju─Źno to─Źko povezave**.
12. Izberite **Ne** in tako dolo─Źite, da povezave ne boste overjali s pomo─Źjo potrdil.
13. Kliknite **Naprej**, da boste odprli stran **Lokalni stre┼żnik klju─Źev**.
14. V polju **Vrsta identifikatorja** izberite **Naslov IP razli─Źice 4**.
15. V polju **Naslov IP** izberite 204.146.18.227.
16. Kliknite **Naprej**, da boste odprli stran **Oddaljeni stre┼żnik klju─Źev**.
17. V polju **Vrsta identifikatorja** izberite **Naslov IP razli─Źice 4**.
18. V polje **Identifikator** vnesite 208.222.150.250.
19. V polje **Klju─Ź z vnaprej dolo─Źeno skupno rabo** vnesite visokozaupen.
20. Kliknite **Naprej**, da boste odprli stran **Lokalna podatkovna zaklju─Źna to─Źka**.
21. V polju **Vrsta identifikatorja** izberite **Podmre┼ža IP razli─Źice 4**.
22. V polje **Identifikator** vnesite 10.6.0.0.
23. V polje **Maska podmre┼że** vnesite 255.255.0.0.
24. Kliknite **Naprej**, da boste odprli stran **Oddaljena podatkovna zaklju─Źna to─Źka**.
25. V polju **Vrsta identifikatorja** izberite **Podmre┼ža IP razli─Źice 4**.

26. V polje **Identifikator** vnesite 10.196.8.0.
27. V polje **Maska podmre┼że** vnesite 255.255.255.0.
28. Kliknite **Naprej**, da boste odprli stran **Podatkovne storitve**.
29. Sprejmite privzete vrednosti, nato pa kliknite **Naprej**, da boste odprli stran **Podatkovno na─Źelo**.
30. Izberite **Izdelaj novo na─Źelo**, nato pa izberite **Uravnote┼żi za┼í─Źito in zmogljivost**. Izberite **Uporabi algoritem ┼íifriranja RC4**.
31. Kliknite **Naprej**, da boste odprli stran **Uporabni vmesniki**.
32. V tabeli **Linija** izberite **TRLINE**.
33. Kliknite **Naprej**, da boste odprli stran **Povzetek**. Preglejte ali so objekti, ki jih bo izdelal ─Źarovnik, pravilni.
34. Za dokon─Źanje konfiguriranja kliknite **Dokon─Źaj**.
35. Ko se prika┼že pogovorno okno **Aktiviranje filtrov na─Źel** izberite **Da, aktiviraj ustvarjene filtre na─Źel**, nato pa izberite **Dovoli ves drug promet**. Za dokon─Źanje konfiguriranja kliknite **Potrdi**. Ko vas program pozove, podajte, da ┼żelite aktivirati pravila za vse vmesnike.

Zdaj ste kon─Źali s konfiguriranjem VPN na iSeries-A. Naslednji korak je konfiguriranje prehoda VPN za ra─Źunovodski oddelek (iSeries-C).

4. korak: Konfigurirajte VPN na iSeries-C

Sledite istim korakom kot smo jih uporabili za konfiguriranje iSeries-A in po potrebi zamenjajte naslov IP. Kot vodilo uporabite na─Źrtovalne preglednice. Ko kon─Źate s konfiguriranjem prehoda VPN za ra─Źunovodski oddelek, bodo povezave v stanju *na zahtevo*, kar pomeni, da se povezava za┼żene, ko so poslani datagrami IP, ki jih mora ┼í─Źititi ta povezava VPN. Naslednji korak je zagon stre┼żnikov VPN, ─Źe ┼íe niso zagnani.

6. korak: Za┼żenite stre┼żnike VPN

Stre┼żnike VPN za┼żenite takole:

1. V Navigatorju iSeries raz┼íirite **stre┼żnik —>Omre┼żje —>Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Za┼żeni**.

7. korak: Preizkusite povezavo

Ko kon─Źate s konfiguriranjem obeh stre┼żnikov in uspe┼íno za┼żenete stre┼żnika VPN, preizkusite povezljivost in zagotovite, da lahko oddaljeni podmre┼żi medsebojno komunicirata. To naredite takole:

1. V Navigatorju iSeries raz┼íirite **iSeries-A —>Omre┼żje**.
2. Z desno tipko mi┼íke kliknite **Konfiguracija TCP/IP** in izberite **Pomo┼żni programi**, nato pa izberite **Ping**.
3. V pogovornem oknu **Ping iz** vnesite v polje **Ping** iSeries-C.
4. Kliknite **Zdaj izvedi Ping**, da boste preverili povezljivost med iSeries-A in iSeries-C.
5. Ko kon─Źate, kliknite **Potrdi**.

Scenarij VPN: Osnovna povezava od podjetja do podjetja

┼átevilna podjetja uporabljajo za nudenje varnih komunikacij med poslovnimi partnerji, podru┼żnicami in prodajalci frame relay ali zakupljeno linijo. Na ┼żalost so te re┼íitve pogosto drage in geografsko omejene. VPN nudi drugo mo┼żnost za podjetja, ki ┼żelijo zasebne in stro┼íkovno ustrezne komunikacije.

Denimo, da ste glavni dobavitelj delov za proizvajalca. Ker je zelo pomembno, da imate dolo─Źene dele in koli─Źine na voljo takrat, kot to zahteva proizvajalec, morate vedno poznati status inventarja proizvajalca in njegove proizvodne urnike. Morda vodite ta postopek ro─Źno, vendar ste ugotovili, da je to zelo zamudno, drago in v─Źasih celo neto─Źno. Najti ┼żelite preprostej┼íi, hitrej┼íi in u─Źinkovitej┼íi na─Źin komuniciranja s podjetjem proizvajalca. Toda ker gre za izmenjavo zaupnih in ─Źasovno ob─Żutljivih informacij, jih proizvajalec ne ┼żeli objaviti na svoji spletni strani ali poslati mese─Źno v zunanjem poro─Żilu. Z uporabo javnega interneta lahko preprosto vzpostavite zasebno navidezno omre┼żje (VPN), ki bo zadostilo potrebam obeh podjetij.

Cilji

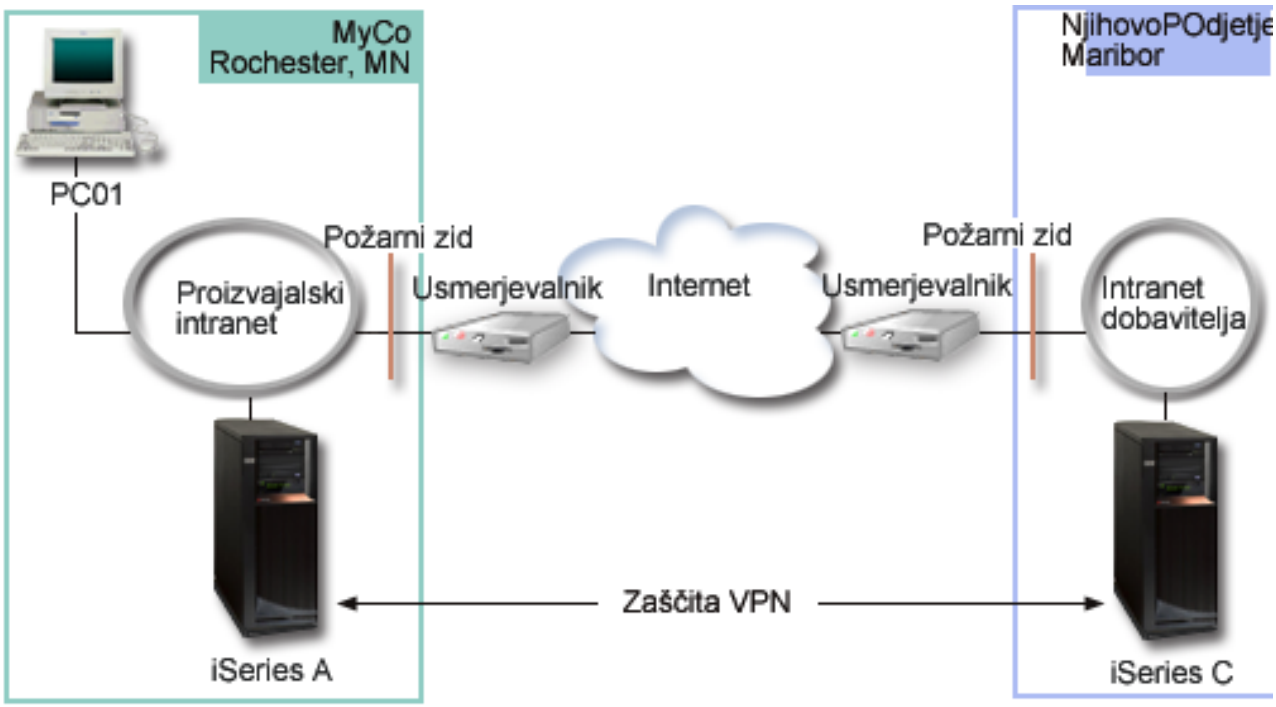
V tem scenariju ┼żeli Mojepodjetje vzpostaviti VPN med gostiteljem v oddelku za dele in gostiteljem v proizvodnem oddelku poslovnega partnerja Njihovopodjetje.

Ker so informacije, ki jih souporabljata ti podjetji, visoko zaupne, morajo biti na poti prek interneta za┼í─Źitene. Poleg tega morajo biti podatki za┼í─Źiteni tudi znotraj omre┼żja vsakega podjetja, saj si omre┼żji ne zaupata. Z drugimi besedami povedano, zahtevata obe podjetji overjanje od enega konca do drugega, integriteto in ┼íifriranje.

Pomembna opomba:
Namen tega scenarija je s pomo─Źjo zgleda prikazati preprosto konfiguracijo VPN od gostitelja do gostitelja. V zna─Źilnem omre┼żnem okolju boste morali med drugim razmisliti tudi o konfiguriranju po┼żarnega zidu, zahtevah za naslavljanje IP in usmerjanju.

Podrobnosti

Naslednja slika ka┼że omre┼żne zna─Źilnosti za Mojepodjetje in Njihovopodjetje:



Omre┼żje dobavitelja Mojepodjetje

- V iSeries-A se izvaja OS/400(R) razli─Źice 5 izdaje 2 (V5R2).
- Naslov IP iSeries-A je 10.6.1.1. To je zaklju─Źna to─Źka povezave, kot tudi podatkovna zaklju─Źna to─Źka. iSeries-C tako izvaja pogajanja IKE in uveljavlja IPSec za vhodne in izhodne datagrame IP in je tudi izvor in cilj podatkov, ki potujejo prek VPN.
- iSeries-A je v podmre┼żi 10.6.0.0 z masko 255.255.0.0
- Povezavo z iSeries-C lahko inicializira samo iSeries-A.

Omre┼żje proizvajalca Njihovopodjetje

- V iSeries-C se izvaja OS/400 razli─Źice 5 izdaje 2 (V5R2).

- Naslov IP iSeries-C je 10.196.8.6. To je zaklju─Źna to─Źka povezave, kot tudi podatkovna zaklju─Źna to─Źka. iSeries-C tako izvaja pogajanja IKE in uveljavlja IPSec za vhodne in izhodne datagrame IP in je tudi izvor in cilj podatkov, ki potujejo prek VPN.
- iSeries-C je v podmre┼żi 10.196.8.0 z masko 255.255.255.0

Konfiguracijske naloge

Za konfiguriranje povezave od podjetja do podjetja morate dokon─Źati vse izmed nalog, opisanih v tem scenariju:

1. Preverite usmerjanje TCP/IP in zagotovite, da lahko komunicirata iSeries-A in iSeries-C prek interneta. To zagotavlja, da bodo gostitelji v vsaki podmre┼żi pravilno izvajali usmeritve v ustrezen prehod za dostop do oddaljene podmre┼že. Ne pozabite, da bo v tem scenariju morda potrebno razmisliti o usmerjanju zasebnih naslovov, ki jih pred tem niste imeli.

   Opomba: Usmerjanje je predmet, ki presega namen te teme. ─Äe imate vpra┼íanja, preberite temo Informacijskega centra z naslovom Usmerjanje TCP/IP in uravnote┼żenje obremenitve.
2. Izpolnite (stran 10) na─Źrtovalne preglednice in potrditvene sezname za oba sistema.
3. Konfigurirajte (stran 11) VPN na iSeries-A v omre┼żju dobavitelja Mojepodjetje.
4. Konfigurirajte (stran 12) VPN na iSeries-C v omre┼żju proizvajalca Njihovopodjetje.
5. Aktivirajte (stran 12) pravila za filtriranje na obeh stre┼żnikih.
6. Za┼żenite (stran 12) povezavo z iSeries-A.
7. Preizkusite (stran 13) komunikacije med oddaljenima podmre┼żama.

Podrobnosti konfiguriranja

Ko dokon─Źate prvi korak in preverite, ali usmerjanje TCP/IP pravilno deluje in stre┼żnika lahko komunicirata, lahko za─Źnete s konfiguriranjem VPN.

2. korak: Izpolnite na─Źrtovalne preglednice

Naslednji na─Źrtovalni potrditveni seznami ka┼żejo vrsto informacij, ki jih potrebujete, preden za─Źnete konfigurirati VPN. Preden za─Źnete z nastavitvijo VPN, morajo biti vsi odgovori na predpogojnem potrditvenem seznamu DA.

Opomba: Te preglednice veljajo za iSeries-A, postopek ponovite tudi za iSeries-C in po potrebi zamenjajte naslov IP.

Predpogojni potrditveni seznam	Odgovori
Ali uporabljate OS/400(R) izdaje V5R2 (5722-SS1) ali novej┼íe?	Da
Ali ste namestili Upravljalnik digitalnih potrdil (mo┼żnost 5722-SS1 34)?	Da
Ali ste namestili ponudnik ┼íifriranega dostopa (5722-AC2 ali AC3)?	Da
Ali ste namestili iSeries(TM) Access za Windows(R) (5722-XE1)?	Da
Ali ste namestili Navigator iSeries Navigator?	Da
Ali ste namestili omre┼żno podkomponento Navigatorja iSeries?	Da
Ali ste namestili pomo┼żne programe TCP/IP za povezljivost za OS/400 (5722-TC1)?	Da
Ali ste nastavili sistemsko vrednost za ohranitev za┼í─Źitnih podatkov stre┼żnika (QRETSVRSEC *SEC) na 1?	Da
Ali je na iSeries konfiguriran TCP/IP (vklju─Źno z vmesniki IP, smermi, imenom lokalnega gostitelja in imenom lokalne domene)?	Da
Ali je med zahtevanima zaklju─Źnima to─Źkama vzpostavljeno obi─Źajno komuniciranje TCP/IP?	Da
Ali ste uveljavili najnovej┼íe za─Źasne popravke programa (PTF-je)?	Da
Ali pravila za filtriranje po┼żarnega zidu ali usmerjevalnika podpirajo protokola AH in ESP, ─Źe pre─Źka tunel VPN po┼żarne zidove ali usmerjevalnike, ki uporabljajo pravila za filtriranje paketov IP?	Da

Predpogojni potrditveni seznam	Odgovori
Ali so po┼žarni zidovi in usmerjevalniki konfigurirani tako, da dopu┼í–Źajo protokole IKE (UDP vrata 500), AH in ESP?	Da
Ali so po┼žarni zidovi konfigurirani tako, da omogo–Źajo odpo┼íiljanje IP?	Da

Te informacije potrebujete za konfiguriranje VPN	Odgovori
Kak┼íno vrsto povezave izdelujete?	Od gostitelja do gostitelja
Kako boste poimenovali skupino dinami–Źnih klju–Źev?	Mojpod2Njihpodj
Kak┼íno vrsto za┼í–Źite in zmogljivosti sistema potrebujete za za┼í–Źito klju–Źev?	Najvi┼íjo
Ali overjate povezavo s pomo–Źjo potrdil? –îe ne, kak┼íen je klju–Ź z vnaprej dolo–Ženo skupno rabo?	Da
Kak┼íen je identifikator lokalnega stre┼żnika klju–Źev?	Naslov IP: 10.6.1.1
Kak┼íen je identifikator lokalne zaklju–Źne podatkovne to–Źke?	Naslov IP: 10.6.1.1
Kak┼íen je identifikator oddaljenega stre┼żnika klju–Źev?	Naslov IP: 10.196.8.6
Kak┼íen je identifikator oddaljene podatkovne zaklju–Źne to–Źke?	Naslov IP: 10.196.8.6
Katera vrata in protokole ┼żelite dovoliti za povezavo?	Katerekoli
Kak┼íno vrsto za┼í–Źite in zmogljivosti sistema potrebujete za za┼í–Źito podatkov?	Najvi┼íjo
Na katere vmesnike se nana┼ía povezava?	TRLINE

3. korak: Konfigurirajte VPN na iSeries-A

S pomo–Źjo informacij iz preglednic konfigurirajte VPN na iSeries-A:

1. V Navigatorju iSeries raz┼íirite stre┼żnik —**>Omre┼żje** —**>Na–Źela IP**.
2. Z desno tipko mi┼íke kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Nova povezava**, da boste zagnali –Źarovnika za povezavo.
3. Na **naslovni** strani si oglejte informacije o objektih, ki jih izdela –Źarovnik.
4. Kliknite **Naprej**, da boste odprli stran **Ime povezave**.
5. V polje **Ime** vnesite Mojpodj2Njihpodj.
6. (izbirno) Podajte opis te povezovalne skupine.
7. Kliknite **Naprej**, da boste odprli stran **Scenarij povezave**.
8. Izberite **Povezava gostitelja z drugim gostiteljem**.
9. Kliknite **Naprej**, da boste odprli stran **Na–Źelo izmenjave internetnih klju–Źev**.
10. Izberite **Izdelaj novo na–Źelo**, nato pa izberite **Najvi┼íja za┼í–Źita, najni┼żja zmogljivost**.
11. Kliknite **Naprej**, da boste odprli stran **Potrdilo za lokalno zaklju–Źno to–Źko povezave**.
12. Izberite **Da** in dolo–Źite, da boste overjali povezavo s pomo–Źjo potrdil. Nato izberite potrdilo, ki predstavlja iSeries-A.
    Opomba: –îe ┼żelite uporabiti potrdilo za overjanje lokalne zaklju–Źne to–Źke povezave, ga morate najprej izdelati v Upravljalniku digitalnih potrdil (DCM).
13. Kliknite **Naprej**, da boste odprli stran **Identifikator lokalne zaklju–Źne to–Źke povezave**.
14. Kot vrsto identifikatorja izberite **Naslov IP razli–Źice 4**. Naslov povezanega naslova IP mora biti 10.6.1.1. Te informacije so definirane v potrdilu, ki ga izdelate v DCM.
15. Kliknite **Naprej**, da boste odprli stran **Oddaljeni stre┼żnik klju–Źev**.
16. V polju **Vrsta identifikatorja** izberite **Naslov IP razli–Źice 4**.
17. V polje **Identifikator** vnesite 10.196.8.6.
18. Kliknite **Naprej**, da boste odprli stran **Podatkovne storitve**.
19. Sprejmite privzete vrednosti, nato pa kliknite **Naprej**, da boste odprl stran **Podatkovno na–Źelo**.

20. Izberite **Izdelaj novo na–Źelo**, nato pa **Najvi┼íja za┼í–Źita, najni┼żja zmogljivost**. Izberite **Uporabi algoritem ┼íifriranja RC4**.
21. Kliknite **Naprej**, da boste odprli stran **Uporabni vmesniki**.
22. Izberite **TRLINE**.
23. Kliknite **Naprej**, da boste odprli stran **Povzetek**. Preglejte ali so objekti, ki jih bo izdelal –Źarovnik, pravilni.
24. Za dokon–Źanje konfiguriranja kliknite **Dokon–Źaj**.
25. Ko se prika┼że pogovorno okno **Aktiviranje filtrov na–Źel**, izberite **Ne, pravila paketov bodo aktivirana kasneje** in kliknite **Potrdi**.

V naslednjem koraku morate podati, da lahko vpelje to povezavo samo iSeries-A. To naredite s prilagoditvijo lastnosti skupine dinami–Źnih klju–Źev Mojpodj2Njihpodj, ki jo je izdelal –Źarovnik:

1. V levem podoknu vmesnika VPN kliknite **Po skupini**; v desnem podoknu se prika┼że skupina dinami–Źnih klju–Źev Mojpodj2Njihpodj. Kliknite jo z desno tipko mi┼íke in izberite **Lastnosti**.
2. Odprite stran **Na–Źelo** in izberite mo┼żnost **Povezavo inicializira lokalni sistem**.
3. S klikom gumba **Potrdi** shranite spremembe.

Zdaj ste kon–Źali s konfiguriranjem VPN na iSeries-A. Naslednji korak je konfiguriranje VPN na iSeries-C v omre┼żju proizvajalca Njihovopodjetje.

4. korak: Konfigurirajte VPN na iSeries-C

Sledite istim korakom kot smo jih uporabili za konfiguriranje iSeries-A in po potrebi zamenjajte naslov IP. Kot vodilo uporabite na–Źrtovalne preglednice. Ko kon–Źate s konfiguriranjem iSeries-C, morate aktivirati pravila za filtriranje, ki jih je izdelal –Źarovnik Povezava na vsakem stre┼żniku.

5. korak: Aktivirajte pravila paketov

–îarovnik samodejno izdela pravila paketov, ki jih zahteva ta povezava za pravilno delovanje. Toda preden lahko za┼żenete povezavo VPN, jih morate aktivirati v obeh sistemih. Na iSeries-A to naredite takole:

1. V Navigatorju iSeries raz┼íirite **iSeries-A —>Omre┼żje —>Na–Źela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Aktiviraj**. Odpre se pogovorno okno **Aktiviranje pravil paketov**.
3. Izberite, ali ┼żelite aktivirati samo pravila, ustvarjena z VPN, samo izbrano datoteko ali pravila, ustvarjena z VPN in izbrano datoteko. Zadnje lahko na primer izberete, –Źe imate me┼íana pravila DOVOLI in ZAVRNI, ki jih ┼żelite uveljaviti za vmesnik poleg pravil, ustvarjenih z VPN.
4. Izberite vmesnik, za katerega ┼żelite aktivirati pravila. V tem primeru izberite **Vsi vmesniki**.
5. V pogovornem oknu kliknite **Potrdi** in potrdite, da ┼żelite preveriti in aktivirati pravila v podanem vmesniku ali vmesnikih. Ko kliknete Potrdi, sistem preveri skladnjo in semanti–Źne napake v pravilih in sporo–Źi rezultate v sporo–Źilnem oknu na dnu urejevalnika. Za sporo–Źila o napakah, ki so povezana z dolo–Źeno datoteko ali ┼ítevilko vrstice, lahko z desno tipko mi┼íke kliknete napako in izberete **Pojdi na vrstico**, da boste ozna–Źili napako v datoteki.
6. Ponovite te korake za aktiviranje pravil paketov na iSeries-C.

6. korak: Za┼żenite povezavo

Naslednji koraki ka┼żejo, kako za┼żenete povezavo Mojpodj2Njihpodj iz iSeries-A:

1. V Navigatorju iSeries raz┼íirite **iSeries-A —>Omre┼żje —>Na–Źela IP**.
2. –îe stre┼żnik VPN ni zagnan, z desno tipko mi┼íke kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Za┼żeni**. S tem za┼żenete stre┼żnik VPN.
3. Raz┼íirite **Delo z zasebnim navideznim omre┼żjem —>Za┼í–Źitene povezave**.
4. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
5. Z desno tipko mi┼íke kliknite **Mojpodj2Njihpodj** in izberite **Za┼żeni**.

6. Z menija **Prikaz** izberite **Osve┼ži**. –še se povezava uspe┼íno za┼žene, se njen status spremeni iz *Mirujo–Ża* v *Omogo–Żena*. Zagon povezave lahko traja nekaj minut, zato jo ob–Żasno osve┼žite, dokler se status ne spremeni v *Omogo–Żena*.

7. korak: Preizkusite povezavo

Ko kon–Żate s konfiguriranjem obeh stre┼žnikov in uspe┼íno za┼ženete povezavo, preizkusite povezljivost in zagotovite, da lahko oddaljena gostitelja komunicirata. To naredite takole:

1. V Navigatorju iSeries raz┼íirite **iSeries-A —>Omre┼žje**.
2. Z desno tipko mi┼íke kliknite **Konfiguracija TCP/IP** in izberite **Pomo┼žni programi**, nato pa izberite **Ping**.
3. V pogovornem oknu **Ping iz** vnesite v polje **Ping** iSeries-C.
4. Kliknite **Zdaj izvedi Ping**, da boste preverili povezljivost med iSeries-A in iSeries-C.
5. Ko kon–Żate, kliknite **Potrdi**.

Scenarij VPN: Za┼í–Żita prostovoljnega tunela L2TP z IPSec

Denimo, da ima va┼íe podjetje majhno podru┼žnico v drugi dr┼žavi. Vse delovni dni potrebuje podru┼žnica dostop do zaupnih informacij na iSeries(TM) znotraj zdru┼ženega intraneta. Va┼íe podjetje trenutno uporablja drago zakupljeno linijo, s pomo–Żjo katere nudi podru┼žnici dostop do zdru┼ženega omre┼žja. –ieprav ┼želi va┼íe podjetje ┼íe naprej nuditi varen dostop do intraneta, ┼želi zmanj┼íati stro┼íke, povezane z zakupljeno linijo. To lahko naredite z izdelavo prostovoljnega tunela L2TP (Layer 2 Tunnel Protocol), ki raz┼íiri zdru┼ženo omre┼žje, tako da postane podru┼žnica del zdru┼žene podmre┼že. VPN ┼í–Żiti promet podatkov prek tunela L2TP.

S prostovoljnim tunelom L2TP vzpostavi oddaljena podru┼žnica tunel neposredno z omre┼žnim stre┼žnikom L2TP (LNS) zdru┼ženega omre┼žja. Funkcionalnost koncentratorja dostopa L2TP (LAC) je na odjemalcu. Tunel je transparenten za ponudnika internetnih storitev oddaljenega odjemalca, zato ni nujno, da ISP podpira L2TP. –ie ┼želite podrobnej┼íe informacije o konceptih L2TP, preberite L2TP (Layer 2 Tunnel Protocol).

> **Pomembna opomba:**
> V tem scenariju sta priklju–Żena za┼í–Żitna prehoda iSeries neposredno v internet. Po┼žarnega zidu nismo vklju–Żili zato, da bi poenostavili scenarij, kar pa ne pomeni, da uporaba po┼žarnega zidu ni potrebna. Razmislite o vseh tveganjih, povezanih z za┼í–Żito, vsaki–Ź ko se pove┼žete v internet. V rde–Żi knjigi AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> boste na┼íli podroben opis razli–Żnih na–Żinov za zmanj┼íanje teh tveganj.

Cilji

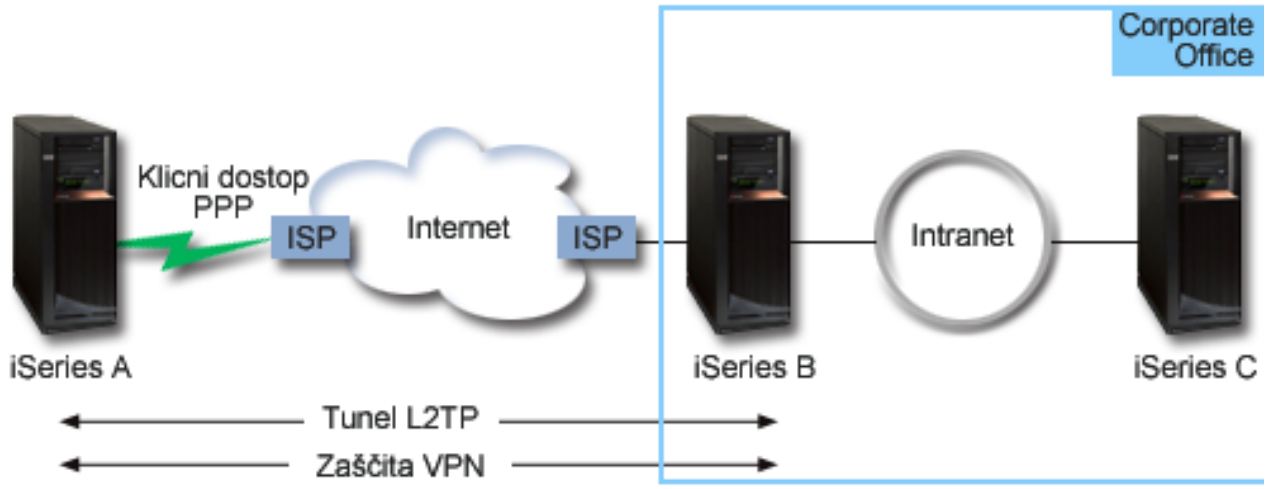
V tem scenariju se pove┼že iSeries podru┼žnice s svojim zdru┼ženim omre┼žjem prek prehodnega iSeries s tunelom L2TP, ki ga ┼í–Żiti VPN.

Glavni cilji tega scenarija so naslednji:

- Sistem podru┼žnice vedno inicializira povezavo z glavno pisarno.
- Sistem podru┼žnice je edini sistem v omre┼žju podru┼žnice, ki potrebuje dostop do zdru┼ženega omre┼žja. Z drugimi besedami povedano ima v omre┼žju podru┼žnice vlogo gostitelja in ne prehoda.
- Zdru┼żeni sistem je ra–Żunalnik gostitelj v zdru┼ženem omre┼žju.

Podrobnosti

Naslednja slika ka┼že omre┼žne zna–Żilnosti za ta scenarij:



iSeries-A

- Mora imeti dostop do aplikacij TCP/IP v vseh sistemih zdru┼ženega omre┼ža.
- Prejme dinami─Źno dodeljene naslove IP od svojega ponudnika internetnih storitev.
- Mora biti konfiguriran tako, da nudi podporo za L2TP.

iSeries-B

- Mora imeti dostop do aplikacij TCP/IP na iSeries-A.
- Podmre┼ža je 10.6.0.0, maska pa 255.255.0.0. Ta podmre┼ža predstavlja podatkovno zaklju─Źno to─Źko tunela VPN v zdru┼ženem mestu.
- V internet se pove┼že z naslovom IP 205.13.237.6. To je zaklju─Źna to─Źka povezave. To pomeni, da izvaja iSeries-B upravljanje klju─Źev in uveljavi IPSec za vhodne in izhodne datagrame IP. iSeries-B se pove┼že s svojo podmre┼žo z naslovom IP 10.6.11.1.

V dolo─Źbah L2TP deluje *iSeries-A* kot pobudnik L2TP, *iSeries-B* pa kot zaklju─Ževalec L2TP.

Konfiguracijske naloge

Pod pogojem, da konfiguracija TCP/IP ┼že obstaja in deluje, morate opraviti naslednje naloge:

1. Konfiguracija VPN (stran 14) na iSeries-A.
2. Konfiguracija profila povezave PPP (stran 16) in navidezne linije za iSeries-A.
3. Uveljavitev (stran 17) skupine dinami─Źnih klju─Źev za profil PPP.
4. Konfiguracija VPN (stran 17) na iSeries-B.
5. Konfiguracija profila povezave PPP (stran 18) in navidezne linije za iSeries-B.
6. Aktiviranje (stran 18) pravil paketov na iSeries-A in iSeries-B.
7. Zagon (stran 19) povezave z iSeries-A.

Podrobnosti konfiguriranja

Ko preverite, ali TCP/IP pravilno deluje in lahko stre┼žniki iSeries(TM) komunicirajo, lahko za─Źnete s konfiguriranjem povezave, opisane v tem scenariju.

1. korak: konfiguriranje VPN na iSeries-A

Naslednji koraki ka┼žejo, kako konfigurirate VPN na iSeries-A:

1. **Konfigurirajte na─Źelo Internet Key Exchange**

a. V Navigatorju iSeries raz┼íirite iSeries-A —> **Omre┼žje** —> **Na─Źela IP** —> **Delo z navideznim zasebnim omre┼žjem** —> **Na─Źela za┼í─Źite IP**.
b. Z desno tipko mi┼íke kliknite **Na─Źela Internet Key Exchange** in izberite **Novo na─Źelo Internet Key Exchange**
c. Na strani **Oddaljeni stre┼żnik** izberite kot tip identifikatorja **Naslov IP razli─Źice 4** in v polje **Naslov IP** vpi┼íite 205.13.237.6.
d. Na strani **Povezave** izberite **Klju─Ź z vnaprej dolo─Ženo skupno rabo**, da boste dolo─Žili, da ta povezava overja to na─Želo s pomo─Źjo klju─Źa z vnaprej dolo─Ženo skupno rabo.
e. V polje **Klju─Ź** vnesite klju─Ź z vnaprej dolo─Ženo skupno rabo. Ta klju─Ź obravnavajte kot geslo.
f. Za tip identifikatorja lokalnega stre┼żnika klju─Źev izberite **Identifikator klju─Źa**, nato pa vnesite identifikator v polje **Identifikator**. Na primer tojeidklju─Źa. Ne pozabite, da je lokalnemu stre┼żniku klju─Źev naslov IP dodeljen dinami─Źno in ga vnaprej ni mogo─Že poznati. iSeries-B s pomo─Źjo tega identifikatorja dolo─Ži iSeries-A, ─Że iSeries-A inicializira povezavo.
g. Na strani **Pretvorbe** kliknite **Dodaj**, da boste dodali pretvorbe, ki jih predlaga iSeries-A iSeries-B za za┼í─Žito klju─Źev, in podali, ali bo na─Želo IKE pri inicializaciji pogajanj prve faze uporabilo za┼í─Žito identitete.
h. Na strani **Pretvorba na─Žela IKE** izberite za na─Žin overjanja **Klju─Ź z vnaprej dolo─Ženo skupno rabo**, **SHA** za razpr┼íilni algoritem in **3DES-CBC** za ┼íifrirni algoritem. Sprejmite privzete vrednosti za skupino Diffie-Hellman in potek klju─Źev IKE.
i. Kliknite **Potrdi**, da se boste vrnili na stran **Pretvorbe**.
j. Izberite **Pogajanja IKE v agresivnem na─Žinu (brez za┼í─Žite identitete).**

Opomba: ─Že morate v konfiguraciji uporabiti klju─Że z vnaprej dolo─Ženo souporabo in pogajanje agresivnega na─Žina, uporabite zapletena gesla, ki jih je zelo te┼żko zlomiti v napadih, ki pregledujejo slovar. Priporo─Ženo je tudi, da redno spreminjate gesla.

k. Kliknite **Potrdi**, da boste shranili konfiguracije.

2. **Konfiguriranje podatkovnega na─Žela**
   a. V vmesniku VPN z desno tipko mi┼íke kliknite **Podatkovna na─Žela** in izberite **Novo podatkovno na─Želo**.
   b. Na strani **Splo┼íno** podajte ime podatkovnega na─Žela. Na primer oddaljeniuporabnikl2tp.
   c. Odprite stran **Predlogi**. Predlog je zbirka protokolov, ki jih uporabljajo pobudni in odzivni stre┼żniki klju─Źev za vzpostavitev dinami─Źne povezave med dvema zaklju─Źnima to─Źkama. Eno podatkovno na─Želo lahko uporabite v ve─Ź povezovalnih objektih, vendar ni nujno, da imajo vsi oddaljeni stre┼żniki klju─Źev VPN iste lastnosti podatkovnih na─Žel. Zato lahko dodate v eno podatkovno na─Želo ve─Ź predlogov. Pri vzpostavitvi povezave VPN z oddaljenim stre┼żnikom klju─Źev mora biti v podatkovnem na─Želu pobudnika in odzivnika vsaj en ujemajo─Ź se predlog.
   d. S klikom gumba **Dodaj** dodajte pretvorbo podatkovnega na─Žela.
   e. Za na─Žin enkapsulacije izberite **Prenos**.
   f. Podajte vrednost za iztek klju─Źa.
   g. Kliknite **Potrdi**, da se boste vrnili na stran **Pretvorbe**.
   h. S klikom gumba **Potrdi** shranite novo podatkovno na─Želo.
3. **Konfiguriranje skupine dinami─Źnih klju─Źev**
4.
   a. V vmesniku VPN raz┼íirite **Za┼í─Žitene povezave**.
   b. Z desno tipko mi┼íke kliknite **Po skupini** in izberite **Nova skupina dinami─Źnih klju─Źev**.
   c. Na strani **Splo┼íno** podajte ime skupine. Na primer l2tpvpodj.
   d. Izberite **┼á─Žiti lokalno inicializiran tunel L2TP**.
   e. Za vlogo sistema izberite **Oba sistema sta gostitelja**.

f. Odprite stran **Na─Źelo**. S spustnega seznama **Podatkovno na─Źelo** izberite podatkovno na─Źelo, ki ste ga izdelali v drugem koraku - oddaljeniuporabnikl2tp.

g. Izberite **Povezavo inicializira lokalni sistem**, in dolo─Źite, da lahko inicializira povezavo z iSeries-B samo iSeries-A.

h. Odprite stran **Povezave**. Izberite **Za to skupino ustvari naslednje pravilo za filtriranje na─Źel**. Kliknite **Urejanje** in definirajte parametre filtra na─Źel.

i. Na strani **Filter na─Źel - Lokalni naslovi** izberite za tip identifikatorja **Identifikator klju─Źev**.

j. Za identifikator izberite identifikator klju─Źev tojeidklju─Źa, ki ste ga definirali v na─Źelu IKE.

k. Odprite stran **Filter na─Źel - Oddaljeni naslovi**. S spustnega seznama **Tip identifikatorja** izberite **Naslov IP razli─Źice 4**.

l. V polje **Identifikator** vnesite 205.13.237.6.

m. Odprite stran **Filter na─Źel - Storitve**. V polji **Lokalna vrata** in **Oddaljena vrata** vnesite 1701. Vrata 1701 so znana vrata za L2TP.

n. S spustnega seznama **Protokol** izberite **UDP**.

o. Kliknite **Potrdi**, da se boste vrnili na stran **Povezave**.

p. Odprite stran **Vmesniki**. Izberite katerokoli linijo ali profil PPP, na katerega se bo nana┼íala ta skupina. Za to skupino ┼íe niste izdelali profila PPP. Ko ga izdelate, morate popraviti lastnosti te skupine, tako da se bo skupina nana┼íala na profil PPP, ki ga boste izdelali v naslednjem koraku.

q. Kliknite **Potrdi**, da boste izdelali skupino dinami─Źnih klju─Źev l2tpvpodj.

Zdaj morate v pravkar izdelano skupino dodati povezavo.

5. **Konfiguriranje povezave dinami─Źnega klju─Źa**

a. V vmesniku VPN raz┼íirite **Po skupini**. S tem boste prikazali seznam vseh skupin dinami─Źnih klju─Źev, ki ste jih konfigurirali na iSeries-A.

b. Z desno tipko mi┼íke kliknite **l2tpvpodj** in izberite **Nova povezava dinami─Źnega klju─Źa**.

c. Na strani **Splo┼íno** lahko podate neobvezen opis povezave.

d. Za oddaljen stre┼żnik klju─Źev izberite za tip identifikatorja **Naslov IP razli─Źice IP**.

e. S spustnega seznama **Naslov IP** izberite 205.13.237.6.

f. Razveljavite izbiro mo┼żnosti **Za┼żeni na zahtevo**.

g. Odprite stran **Lokalni naslovi**. Za tip identifikatorja izberite **Identifikator klju─Źa** in s spustnega seznama **Identifikator** izberite tojeidklju─Źa.

h. Odprite stran **Oddaljeni naslovi**. Za tip identifikatorja izberite **Naslov IP razli─Źice 4**.

i. V polje **Identifikator** vnesite 205.13.237.6.

j. Odprite stran **Storitve**. V polji **Lokalna vrata** in **Oddaljena vrata** vnesite 1701. Vrata 1701 so znana vrata za L2TP.

k. S spustnega seznama **Protokol** izberite **UDP**.

l. Kliknite **Potrdi**, da boste izdelali povezavo dinami─Źnega klju─Źa.

Zdaj ste kon─Źali s konfiguriranjem VPN na iSeries-A. Naslednji korak je konfiguriranje profila PPP za iSeries-A.

2. korak: konfiguriranje profila povezave PPP in navidezne linije na iSeries-A

Razdelek opisuje korake, ki jih morate opraviti za izdelavo profila PPP za iSeries-A. S profilom PPP ni povezana nobena fizi─Źna linija, saj namesto nje uporablja navidezno linijo. Razlog za to je, da potuje promet PPP prek tunela L2TP, pri tem pa tunel L2TP ┼í─Źiti VPN.

Profil povezave PPP za iSeries-A izdelate takole:

1. V Navigatorju iSeries raz┼íirite iSeries-A —**>Omre┼żje—>Storitve oddaljenega dostopa**.
2. Z desno tipko mi┼íke kliknite **Profili povezave pobudnika** in izberite **Nov profil**.
3. Na strani **Nastavitev** izberite za tip protokola**PPP**.

4. Za na─Źin izberite **L2TP (navidezna linija)**.
5. S spustnega seznama **Na─Źin delovanja** izberite **Pobudnik na zahtevo (prostovoljen tunel)**.
6. Kliknite **Potrdi**, da boste odprli strani z lastnostmi profilov PPP.
7. Na strani **Splo┼íno** vnesite ime, ki dolo─Ża tip in cilj povezave. V tem primeru vnesite vPODJ. Ime, ki ga podate, je lahko sestavljeno iz najve─Ź 10 znakov.
8. (neobvezno) Podajte opis profila.
9. Odprite stran **Povezava**.
10. V polju **Ime navidezne linije** izberite s spustnega seznama izbiro **vpodj**. Ne pozabite, da ni s to linijo povezan noben fizi─Żen vmesnik. Navidezna linija opisuje razli─Źne zna─Żilnosti tega profila PPP: na primer najve─Żjo dovoljeno velikost okvirja, informacije o overjanju, ime lokalnega gostitelja itd. Odpre se pogovorno okno **Lastnosti linije L2TP**.
11. Na strani **Splo┼íno** vnesite opis navidezne linije.
12. Odprite stran **Overjanje**.
13. V polje **Ime lokalnega gostitelja** vnesite gostiteljsko ime lokalnega stre┼żnika klju─Źev iSeriesA.
14. Kliknite **Potrdi**, da boste shranili nov opis navidezne linije in se vrnili na stran **Povezava**.
15. V polje **Naslov zaklju─Źne to─Źke oddaljenega tunela** vnesite naslov zaklju─Źne to─Źke oddaljenega tunela 205.13.237.6.
16. Izberite **Zahteva za┼í─Żito IPSec** in s spustnega seznama **Povezava** izberite skupino dinami─Źnih klju─Źev, ki ste jo izdelali v prvem koraku - l2tpvpodj.
17. Odprite stran **Nastavitve TCP/IP**.
18. V razdelku **Lokalni naslov IP** izberite **Dodeli oddaljeni sistem**.
19. V razdelku **Oddaljeni naslov IP** izberite **Uporabi stalni naslov IP**. Vnesite 10.6.11.1, ki je naslov IP oddaljenega sistema v njegovi podmre┼ži.
20. V razdelku usmerjanja izberite **Definiraj dodatne stati─Źne smeri** in kliknite **Smeri**. ─Če ni v profilu PPP nobenih informacij o usmerjanju, bo iSeries-A lahko dosegel samo zaklju─Źno to─Źko oddaljenega sistema, vendar nobenega drugega sistema v podmre┼ži 10.6.0.0.
21. Kliknite **Dodaj**, da boste dodali postavko stati─Źne smeri.
22. Vnesite podmre┼żo 10.6.0.0 in masko podmre┼že 255.255.0.0, da boste usmerili ves promet 10.6.*.* prek tunela L2TP.
23. Kliknite **Potrdi**, da boste dodali stati─Źno smer.
24. S klikom gumba **Potrdi** zaprite pogovorno okno Usmerjanje.
25. Odprite stran **Overjanje** in nastavite ime uporabnika in geslo za ta profil PPP.
26. V razdelku Identifikacija lokalnega sistema izberite **Dopusti, da oddaljeni sistem preveri identiteto tega sistema**.
27. Pod razdelkom **Protokol overjanja za uporabo** izberite **Zahtevano ┼íifrirano geslo (CHAP-MD5)**
28. Vnesite ime uporabnika iSeriesA in geslo.
29. S klikom gumba **Potrdi** shranite profil PPP.

3. korak: uveljavitev skupine dinami─Źnih klju─Źev l2tpvpodj za profil PPP vPodj

Ko konfigurirate profil povezave PPP, se morate vrniti v izdelano skupino dinami─Źnih klju─Źev l2tpvpodj in jo povezati s profilom PPP. To naredite takole:

1. Pomaknite se do vmesnika VPN in raz┼íirite **Za┼í─Żitene povezave ──>Po skupini**.
2. Z desno tipko mi┼íke kliknite skupino dinami─Źnih klju─Źev l2tpvpodj in izberite **Lastnosti**.
3. Odprite stran **Vmesniki** iz izberite **Uveljavi to skupino** za profil PPP, ki ste ga izdelali v drugem koraku - vPodj.
4. S klikom gumba **Potrdi** uveljavite l2tpvpodj za profil PPP vPodj.

4. korak: konfiguriranje VPN na iSeries-B

Uporabite iste korake kot pri konfiguriranju iSeries-A in po potrebi zamenjajte naslove IP in identifikatorje. Preden za┼Źnete, razmislite ┼íe o naslednjem:

- Dolo┼Źite oddaljeni stre┼żnik klju┼Źev z identifikatorjem klju┼Źa, ki ste ga podali za lokalni stre┼żnik klju┼Źev na iSeries-A. Na primer tojeidklju┼Źa.
- Uporabite *popolnoma* enak klju┼Ź z vnaprej dolo┼Źeno skupno rabo.
- Preverite, ali se pretvorbe ujemajo s tistimi, ki ste jih konfigurirali na iSeries-A, sicer povezave ne bodo uspele.
- Na strani **Splo┼íno** skupine dinami┼Źnih klju┼Źev ne podajte mo┼żnosti **┼á┼Źiti lokalno inicializiran tunel L2TP**.
- Oddaljeni sistem inicializira povezavo.
- Podajte, naj se povezava za┼żene na zahtevo.

5. korak: konfiguriranje profila povezave PPP in navidezne linije na iSeries-B

Profil povezave PPP za iSeries-B izdelate takole:

1. V Navigatorju iSeries raz┼íirite iSeries-B **—>Omre┼żje—> Storitve oddaljenega dostopa**.
2. Z desno tipko mi┼íke kliknite **Profili povezave odzivnika** in izberite **Nov profil**.
3. Na strani **Nastavitev** izberite za tip protokola**PPP**.
4. Za na┼Źin izberite **L2TP (navidezna linija)**.
5. S spustnega seznama **Na┼Źin delovanja** izberite **Zaklju┼Źevalec (omre┼żni stre┼żnik)**.
6. Na straneh z lastnostmi profilov PPP kliknite **Potrdi**.
7. Na strani **Splo┼íno** vnesite ime, ki dolo┼Źa tip in cilj povezave. V tem primeru vnesite vpodru. Ime, ki ga podate, je lahko sestavljeno iz najve┼Ź 10 znakov.
8. (neobvezno) Podajte opis profila.
9. Odprite stran **Povezava**.
10. Izberite naslov IP lokalne zaklju┼Źne to┼Źke tunela 205.13.237.6.
11. V polju **Ime navidezne linije** izberite s spustnega seznama **vpodru**. Ne pozabite, da ni s to linijo povezan noben fizi┼Źen vmesnik. Navidezna linija opisuje razli┼Źne zna┼Źilnosti tega profila PPP: na primer najve┼Źjo dovoljeno velikost okvirja, informacije o overjanju, ime lokalnega gostitelja itd. Odpre se pogovorno okno **Lastnosti linije L2TP**.
12. Na strani **Splo┼íno** vnesite opis navidezne linije.
13. Odprite stran **Overjanje**.
14. V polje **Ime lokalnega gostitelja** vnesite gostiteljsko ime lokalnega stre┼żnika klju┼Źev iSeriesB.
15. Kliknite **Potrdi**, da boste shranili nov opis navidezne linije in se vrnili na stran **Povezava**.
16. Odprite stran **Nastavitve TCP/IP**.
17. V razdelku **Lokalni naslov IP** izberite stalni naslov IP lokalnega sistema 10.6.11.1.
18. V razdelku **Oddaljeni naslov IP** izberite **Podro┼Źje naslovov** kot na┼Źin za dodeljevanje naslovov. Vnesite za┼Źetni naslov, nato pa podajte ┼ítevilo naslovov, ki jih je mogo┼Źe dodeliti oddaljenemu sistemu.
19. Izberite **Dopusti oddaljenemu sistemu dostop do drugih omre┼żij (odpo┼íiljanje IP)**.
20. Odprite stran **Overjanje** in nastavite ime uporabnika in geslo za ta profil PPP.
21. V razdelku Identifikacija lokalnega sistema izberite **Dopusti, da oddaljeni sistem preveri identiteto tega sistema**. S tem boste odprli pogovorno okno **Identifikacija lokalnega sistema**.
22. Pod razdelkom **Protokol overjanja za uporabo** izberite **Zahtevano ┼íifrirano geslo (CHAP-MD5)**
23. Vnesite ime uporabnika iSeriesB in geslo.
24. S klikom gumba **Potrdi** shranite profil PPP.

6. korak: aktiviranje pravil paketov

VPN samodejno izdela pravila paketov, ki jih zahteva ta povezava za pravilno delovanje. Toda preden lahko za┼żenete povezavo VPN, jih morate aktivirati v obeh sistemih. Na iSeries-A to naredite takole:

1. V Navigatorju iSeries raz┼íirite **iSeries-A —>Omre┼žje —>Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Aktiviraj**. Odpre se pogovorno okno **Aktiviranje pravil paketov**.
3. Izberite, ali ┼żelite aktivirati samo pravila, ustvarjena z VPN, samo izbrano datoteko ali pravila, ustvarjena z VPN in izbrano datoteko. Zadnje lahko na primer izberete, ─Će imate me┼íana pravila DOVOLI in ZAVRNI, ki jih ┼żelite uveljaviti za vmesnik poleg pravil, ustvarjenih z VPN.
4. Izberite vmesnik, za katerega ┼żelite aktivirati pravila. V tem primeru izberite **Vsi vmesniki**.
5. V pogovornem oknu kliknite **Potrdi** in potrdite, da ┼żelite preveriti in aktivirati pravila v podanem vmesniku ali vmesnikih. Ko kliknete Potrdi, sistem preveri skladnjo in semanti─Źne napake v pravilih in sporo─Źi rezultate v sporo─Źilnem oknu na dnu urejevalnika. Za sporo─Źila o napakah, ki so povezana z dolo─Ženo datoteko ali ┼ítevilko vrstice, lahko z desno tipko mi┼íke kliknete napako in izberete **Pojdi na vrstico**, da boste ozna─Źili napako v datoteki.
6. Te korake ponovite ┼íe za aktiviranje pravil paketov na iSeries-B.

7. korak: zagon povezave

Zadnji korak je zagon povezave. Preden lahko inicializirate povezavo L2TP, morate omogo─Źiti zaklju─Ževalec L2TP, da se bo lahko odzival na zahteve pobudnika. Ko se prepri─Žate, da so vse zahtevane storitve zagnane, za┼żenite povezavo PPP na strani zaklju─Ževalca. Naslednji koraki opisujejo, kako zagnati povezavo PPP na iSeries-B:

1. V Navigatorju iSeries raz┼íirite iSeries-B **—> Omre┼žje—> Storitve oddaljenega dostopa**.
2. Kliknite **Profili povezav odzivnika**, da boste v desnem podoknu prikazali seznam profilov odzivnika.
3. Z desno tipko mi┼íke kliknite vpodru in izberite **Za┼żeni**. Ko se profil povezave za┼żene, se okno osve┼ži in prika┼že stanje povezave kot ─Źakanje na povezovalne zahteve. iSeries-A se lahko zdaj odziva na povezovalne zahteve L2TP z iSeries-B.

Naslednji koraki ka┼żejo, kako za┼żenete povezavo L2TP na iSeries-A:

1. V Navigatorju iSeries raz┼íirite iSeries-A **—> Omre┼žje—> Storitve oddaljenega dostopa**.
2. Kliknite **Profili povezav pobudnika**, da boste v desnem podoknu prikazali seznam profilov pobudnika.
3. Z desno tipko mi┼íke kliknite **vPODJ** in izberite **Za┼żeni**. Ko se profil povezave za┼żene, se okno osve┼ži in prika┼že stanje povezave kot Vzpostavljanje tunela L2TP.
4. S tipko F5 lahko osve┼żite zaslon. ─Źe se je tunel L2TP uspe┼íno zagnal, bo status povezave zdaj Aktivne povezave.

Scenarij VPN: uporaba prevoda omre┼żnega naslova za VPN

Denimo, da ste skrbnik omre┼żja v majhnem proizvodnem podjetju v Mariboru. Eden izmed va┼íih poslovnih partnerjev, dobavitelj delov iz Kranja, ┼żeli ve─Źji del poslovanja z vami izvajati prek interneta. Pomembno je, da imate v podjetju dolo─Žene dele in koli─Źine na voljo takrat, ko jih potrebujete, zato mora dobavitelj poznati inventar podjetja in proizvodne urnike. Trenutno izvajate ta postopek ro─Źno, toda ugotovili ste, da je to zamudno, drago in v─Źasih celo neto─Źno, zato ste pripravljeni raziskati nove mo┼żnosti.

Glede na zaupnost informacij, ki jih izmenjate, se odlo─Źite za izdelavo VPN med omre┼żjem dobavitelja in omre┼żjem va┼íega podjetja. Za nadaljnjo za┼í─Źito zasebnosti omre┼żne strukture podjetja se odlo─Źite, da boste skrili zasebni naslov IP iSeries(TM), ki gosti aplikacije, do katerih ima dostop dobavitelj. Vpra┼íanje je, kako to narediti.

Odgovor je uporaba OS/400(R) VPN. Uporabite ga ne le za izdelavo definicij povezav na prehodu VPN v omre┼żju va┼íega podjetja, pa─Ź pa tudi za prevajanje naslovov, potrebno za skritje lokalnih zasebnih naslovov. Za razliko od obi─Zajnega prevoda omre┼żnega naslova (NAT), ki spremeni naslove IP v dogovorih za za┼í─Źito (SA-jih), izvede VPN NAT prevod naslova pred preverjanjem veljavnosti SA, tako da dodeli naslov povezavi pri njenem zagonu.

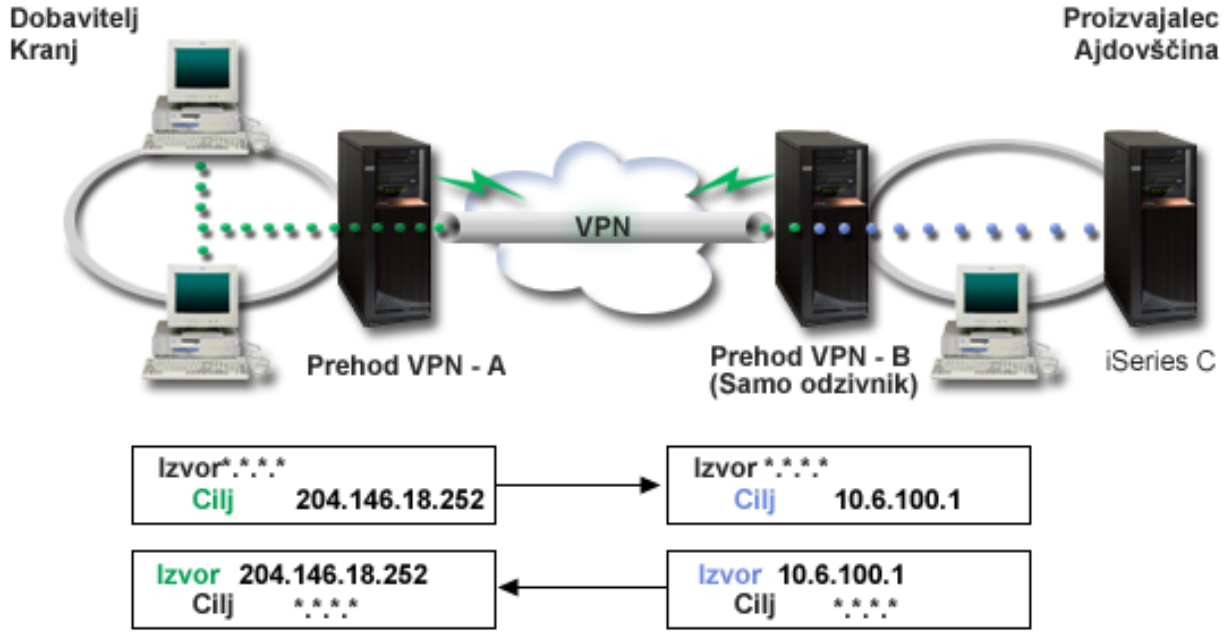
Cilji

Cilji tega scenarija so naslednji:

- vsem odjemalcem v omre┼žju dobavitelja omogo─Źiti dostop do gostitelja iSeries v omre┼žju proizvajalca prek povezave VPN od prehoda do prehoda
- skriti zasebni naslov IP iSeries gostitelja v omre┼žju proizvajalca z njegovim prevodom v javni naslov IP s pomo─Źjo prevoda omre┼żnega naslova za VPN (VPN NAT)

Podrobnosti

Naslednji diagram ka┼že omre┼żne zna─Źilnosti za omre┼žje dobavitelja in za omre┼žje proizvajalca:



- Prehod VPN A je konfiguriran tako, da vedno inicializira povezave s prehodom VPN B.
- Prehod VPN A definira ciljno zaklju─Źno to─Źko za povezavo kot 204.146.18.252 (javni naslov, dodeljen iSeries-C).
- iSeries-C ima zasebni naslov IP v omre┼žju proizvajalca 10.6.100.1.
- Javni naslov 204.146.18.252 je bil definiran v lokalnem storitvenem podro─Źju prehoda VPN B za zasebni naslov iSeries C 10.6.100.1.
- Prehod VPN B prevede javni naslov iSeries C v njegov zasebni naslov 10.6.100.1 za vhodne datagrame. Prehod VPN B prevede vra─Źajo─Że se izhodne datagrame iz 10.6.100.1 nazaj v javni naslov iSeries C 204.146.18.252. Kar se ti─Że odjemalcev v omre┼žju dobavitelja ima iSeries C naslov IP 204.146.18.252, in nikoli ne vedo, da je pri┼ílo do prevoda naslova.

Konfiguracijske naloge

Za konfiguriranje povezave kot je opisano v tem scenariju, morate izpolniti naslednje naloge:

1. Konfigurirati osnovni VPN od prehoda do prehoda med **prehodom VPN A** in **prehodom VPN B**.
2. Definirati lokalno storitveno podro─Źje za **prehod VPN B**, da skrijete zasebni naslov **iSeries-C** za javni identifikator 204.146.18.252.
3. Konfigurirati **prehod VPN B**, da prevedete lokalne naslove s pomo─Źjo naslovov iz lokalnega storitvenega podro─Źja.

Koncepti VPN

Delo z zasebnim navideznim omre┼žjem (VPN) uporablja za za┼í─Źito prometa podatkov ┼ítevilne pomembne protokole TCP/IP. Da bi bolje razumeli, kako deluje povezava VPN, morate poznati te protokole in koncepte in kako jih uporablja OS/400(R) VPN:

- **Protokoli IPSec (IP Security)**
  IPSec nudi stabilno in dolgotrajno osnovo za nudenje za┼í─Źite v omre┼żni plasti.
- **Upravljanje klju─Źev**
  Dinami─Źni VPN nudi dodatno za┼í─Źito komunikacij s pomo─Źjo protokola IKE (Internet Key Exchange) za upravljanje klju─Źev. IKE omogo─Ża, da stre┼żnika VPN na obeh koncih povezave dogovorita nove klju─Że v podanih intervalih.
- **L2TP (Layer 2 Tunneling Protocol)**
  ─Źe nameravate za┼í─Źititi komunikacije med omre┼żjem in oddaljeni odjemalci s pomo─Źjo povezave VPN, morate poznati tudi L2TP.
- **Prevod omre┼żnega naslova za VPN (VPN NAT)**
  VPN OS/400 nudi sredstva za izvedbo prevoda omre┼żnega naslova, imenovana VPN NAT. VPN NAT se razlikuje od obi─Żajnega NAT, saj prevede naslove, preden uveljavi protokola IKE in IPSec. Podrobnej┼íe informacije boste na┼íli v tej temi.
- **Enkapsulacija UDP**
  Enkapsulacija UDP omogo─Ża, da promet IPSec potuje prek obi─Żajne naprave NAT. V tej temi poi┼í─Źite podrobnej┼íe informacije o enkapsulaciji in zakaj bi jo uporabili za povezave VPN.
- **Stiskanje IP (IPComp)**
  IPComp s pomo─Źjo stiskanja zmanj┼ía velikost datagramov IP in tako pove─Ża komunikacijsko zmogljivost med dvema partnerjema VPN.
- **VPN in filtriranje IP**
  Filtriranje IP in VPN sta tesno povezana. Pravzaprav ve─Żina povezav VPN zahteva za pravilno delovanje pravila za filtriranje. Tema vsebuje informacije o tem, katere filtre zahteva VPN, kot tudi druge koncepte filtriranja, povezane z VPN.

Protokoli IPSec (IP Security)

IPSec nudi stabilno in dolgotrajno osnovo za nudenje za┼í─Źite v omre┼żni plasti. Podpira vse algoritma ┼íifriranje, ki so v uporabi, in se lahko prilagodi tudi novej┼íim, mo─Żnej┼íim algoritmom. Protokoli IPSec obravnavajo naslednje glavne predmete v zvezi z za┼í─Źito:

Overjanje izvora podatkov
Preveri, ali vsak datagram v resnici izvira od predstavljenega po┼íiljatelja.
Integriteta podatkov
Preveri, da vsebina datagrama na poti ni bila spremenjena, in sicer namerno ali zaradi naklju─Żnih napak.
Zaupnost podatkov
Skrije vsebino sporo─Żila, obi─Żajno s pomo─Źjo ┼íifriranja.
Za┼í─Źita pred vnovi─Żnim predvajanjem
Zagotavlja, da napadalec ne more prestre─Źi datagrama in ga kasneje znova predvajati.
Samodejno upravljanje ┼íifrirnih klju─Źev in dogovorov za za┼í─Źito
Zagotavlja, da je mogo─Że uporabiti na─Żelo VPN v celotnem raz┼íirjenem omre┼żju z malo ali skoraj ni─Ź ro─Żnega konfiguriranja.

VPN uporablja za za┼í─Źito podatkov pri prehodu skozi VPN dva protokola IPSec: AH (Authentication Header) in ESP (Encapsulating Security Payload). Drugi del omogo─Żitve IPSec je protokol IKE (Internet Key Exchange) ali upravljanje klju─Źev. IPSec ┼íifrira podatke, IKE pa podpira samodejno pogajanje dogovorov za za┼í─Źito (SA-jev), in samodejno tvorbo in osve┼żitev ┼íifrirnih klju─Źev.

Spodaj so navedeni glavni protokoli IPSec:

- **Protokol AH (Authentication Header)**
- **Protokol ESP (Encapsulating Security Payload)**
- **Zdru┼żitev protokolov AH in ESP**
- **Protokol IKE (Internet Key Exchange)**

IETF (Internet Engineering Task Force) formalno definira IPSec v RFC-ju (Request for Comment) 2401, *Security Architecture for the Internet Protocol*. RFC si lahko ogledate na naslednji spletni strani: http://www.rfc-editor.org

.

Protokol Authentication Header

Protokol AH (Authentication Header) omogo─Źa overjanje izvora podatkov, integritete podatkov in za┼í─Źito pred vnovi─Źnim predvajanjem. Toda AH ne omogo─Źa zaupnosti podatkov, kar pomeni, da so vsi poslani podatki jasno vidni.

AH zagotavlja integriteto podatkov s pomo─Źjo nadzorne vsote, ki jo ustvari koda za overjanje sporo─Źila, kot je MD5. Za overjanje izvora podatkov vklju─Źuje AH tajni klju─Ź v skupni rabi v algoritmu, ki ga uporablja za overjanje. Za za┼í─Źito pred vnovi─Źnim predvajanjem uporablja AH polje zaporedne ┼ítevilke znotraj oglavja AH. Tu moramo poudariti, da so te tri lo─Źene funkcije pogosto zdru┼żene in se skupaj imenujejo **overjanje**. Preprosto povedano AH zagotavlja, da na poti do kon─Źnega cilja ni pri┼ílo do vdora.

─ŹeprAv overi AH ─Źim ve─Źji del datagrama IP, sprejemnik ne more predvideti vrednosti dolo─Źenih polj v oglavju IP. AH ne ┼í─Źiti teh polj, ki se imenujejo **spremenljiva**. Toda AH vedno ┼í─Źiti tovor paketa IP.

IETF (Internet Engineering Task Force) formalno definira AH v RFC-ju (Request for Comment) 2402, *IP Authentication Header*. RFC si lahko ogledate na naslednji spletni strani: http://www.rfc-editor.org

.

Na─Źini za uporabo AH

AH lahko uveljavite na dva na─Źina: na─Źin prenosa in na─Źin tunela. V na─Źinu prenosa je oglavje IP datagrama najoddaljenej┼íe oglavje IP, ki mu sledi oglavje AH, nato pa tovor datagrama. AH overi celoten datagram, razen spremenljivih polj. Toda informacije, vsebovane v datagramu, so prenesene neza┼í─Źitene, in zato obstaja mo┼żnost prislu┼íkovanja. Na─Źina prenosa zahteva manj dodatne obremenitve kot na─Źin tunela, toda ne nudi toliko za┼í─Źite.

Na─Źin tunela izdela novo oglavje IP in ga uporabi kot najoddaljenej┼íe oglavje IP datagrama. Oglavje AH sledi novemu oglavju IP. Izvirni datagram (oglavje IP in izvirni tovor) pride na koncu. AH overi celoten datagram, kar pomeni, da lahko odzivni sistem odkrije, ali je bil datagram pri prenosu spremenjen.

─Źe je katerikoli konec dogovora za za┼í─Źito prehod, uporabite na─Źin tunela. V na─Źinu tunela nista izvorni in ciljni naslov v najoddaljenej┼íem oglavju IP ista kot tista v izvirnem oglavju IP. Tako lahko na primer dva za┼í─Źitna prehoda vodita tunel AH za overjanje vsega prometa med omre┼żji, ki ju povezujeta. Pravzaprav je to zelo zna─Źilna konfiguracija.

Glavna prednost uporabe na─Źina tunela je, da na─Źin tunela v celoti ┼í─Źiti enkapsuliran datagram IP. Poleg tega omogo─Źa na─Źin tunela mo┼żnost za uporabo zasebnih naslovov.

Zakaj AH?

V ┼ítevilnih primerih zahtevajo va┼íi podatki samo overjanje. Protokol ESP (Encapsulating Security Payload) lahko izvaja overjanje, toda AH ne vpliva na zmogljivost sistema tako kot ESP. ┼áe ena prednost uporabe AH je, da AH overi celoten datagram. Toda ESP ne overi glavnega oglavja IP ali katerihkoli drugih informacij pred oglavjem ESP.

ESP poleg tega zahteva za uveljavitev mo─Źne algoritme ┼íifriranja. Mo─Źno ┼íifriranje je v nekaterih dr┼żavah omejeno, toda AH ni predpisan in ga lahko kjerkoli svobodno uporabljate.

Katere algoritme uporablja AH za za┼í─Źito informacij?

AH uporablja algoritme, imenovane **hashed message authentication codes (HMAC)**. VPN uporablja HMAC-MD5 ali HMAC-SHA. MD5 in SHA izdelata izhodne podatke s stalno dol┼żino (imenovane razpr┼íilna vrednost) iz vhodnih

podatkov s spremenljivo dol┼žino in tajnega klju─Ża. ─îe se deli dveh sporo─Żil ujemajo, je zelo mogo─Że, da sta sporo─Żili enaki. MD5 in SHA kodirata dol┼žino sporo─Żila v svojih izhodnih podatkih, toda SHA je bolj varen, saj izdela ve─Źje dele.

IETF (Internet Engineering Task Force) formalno definira HMAC-MD5 v RFC-ju (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. IETF (Internet Engineering Task Force) formalno definira HMAC-SHA v RFC-ju (Request for Comments) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC-ja si lahko ogledate na naslednji spletni strani: http://www.rfc-editor.org

.

Protokol ESP (Encapsulating Security Payload)

Protokol ESP (Encapsulating Security Payload) omogo─Źa zaupnost podatkov, izbirno pa nudi tudi overjanje izvora podatkov, preverjanje integritete podatkov in za┼í─Żito pred vnovi─Źnim predvajanjem. Razlika med protokolom ESP in protokolom Authentication Header (AH) je v tem, da nudi ESP ┼íifriranje, med tem ko nudita oba protokola overjanje, preverjanje integritete in za┼í─Żito pred vnovi─Źnim predvajanjem. Z ESP uporabljata oba komunicirajo─Źa sistema za ┼íifriranje in de┼íifriranje podatkov, ki jih izmenjata, klju─Ż v skupni rabi.

─îe se odlo─Żite, da boste uporabili ┼íifriranje in overjanje, potem odzivni sistem najprej overi paket, nato pa, ─Że prvi korak uspe, nadaljuje s de┼íifriranjem. Ta vrsta konfiguracije zmanj┼ía dodatno obremenitev pri obdelavi, kot tudi ranljivost pred napadi z zavrnitvijo storitev.

Dva na─Żina za uporabo ESP

ESP lahko uveljavite na dva na─Żina: na─Żin prenosa in na─Żin tunela. V na─Żinu prenosa sledi oglavje ESP oglavju IP izvirnega datagrama IP. ─îe ima datagram ┼że oglavje IPSec, pride oglavje ESP pred njim. Zaklju─Żek ESP in izbirni podatki overjanja sledijo tovoru.

Na─Żin prenosa ne overja ali ┼íifrira oglavja IP, ker bi lahko s tem pri prehodu datagrama izpostavil informacije o naslovih mo┼żnim napadalcem. Na─Żina prenosa zahteva manj dodatne obremenitve kot na─Żin tunela, toda ne nudi toliko za┼í─Żite. V ve─Żini primerov uporabljajo gostitelji ESP v na─Żinu prenosa.

Na─Żin tunela izdela novo oglavje IP in ga uporabi kot najoddaljenej┼íe oglavje IP datagrama; za njim sledi oglavje ESP, nato pa izvirni datagram (oglavje IP in izvirni tovor). Tovoru sta pripeta zaklju─Żek ESP in izbirni podatki overjanja. ─îe uporabite ┼íifriranje in overjanje, ESP v celoti za┼í─Żiti izvirni datagram, ker postane podatek tovora za nov paket ESP. Toda ESP ne za┼í─Żiti novega oglavja IP. Prehodi morajo uporabiti ESP v na─Żinu tunela.

Katere algoritme uporablja ESP za za┼í─Żito informacij?

ESP uporablja simetri─Żni klju─Ż, ki ga uporabljata obe komunicirajo─Źi stranki za ┼íifriranje in de┼íifriranje podatkov, ki jih izmenjata. Oddajnik in sprejemnik se morata dogovoriti o klju─Żu, preden so lahko vzpostavljene za┼í─Żitene komunikacije. OS/400(R) VPN uporablja za ┼íifriranje DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 ali AES (Advanced Encryption Standard).

IETF (Internet Engineering Task Force) formalno definira DES v RFC-ju (Request for Comment 1829, *The ESP DES-CBC Transform*. IETF (Internet Engineering Task Force) formalno definira 3DES v RFC-ju 1851, *The ESP Triple DES Transform*. Tega in druge RFC-je si lahko ogledate na naslednji spletni strani: http://www.rfc-editor.org

.

ESP omogo─Źa funkcije overjanja s pomo─Żjo algoritmov HMAC-MD5 in HMAC-SHA. MD5 in SHA izdelata izhodne podatke s stalno dol┼žino (imenovane razpr┼íilna vrednost) iz vhodnih podatkov s spremenljivo dol┼žino in tajnega klju─Ża. ─îe se deli dveh sporo─Żil ujemajo, je zelo mogo─Że, da sta sporo─Żili enaki. MD5 in SHA kodirata dol┼žino sporo─Żila v svojih izhodnih podatkih, toda SHA je bolj varen, saj izdela ve─Źje dele.

IETF (Internet Engineering Task Force) formalno definira HMAC-MD5 v RFC-ju (Request for Comments) 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. IETF (Internet Engineering Task Force) formalno definira HMAC-SHA v RFC-ju (Request for Comments) 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Tega in druge RFC-je si lahko ogledate na naslednji spletni strani: http://www.rfc-editor.org

.

Zdru┼żena AH in ESP

VPN omogo─Ża, da zdru┼żite AH in ESP za povezave od gostitelja do gostitelja v prenosnem na─Żinu. Z zdru┼żitvijo teh protokolov za┼í─Żitite celoten datagram IP. ─îeprav nudi zdru┼żitev dveh protokolov ve─Ź za┼í─Żite, lahko dodatna obremenitev pri obdelavi prevlada nad prednostmi.

Upravljanje klju─Źev

Stre┼żniki VPN pri vsakem uspe┼ínem pogajanju na novo ustvarijo klju─Że, ki ┼í─Żitijo povezavo, s ─Żimer napadalcem prepre─Żujejo zajetje informacij iz povezave. ─îe uporabite popolno tajnost, napadalci ne morejo na osnovi starih informacij o klju─Żih izpeljati novih.

Upravljalnik klju─Źev VPN je IBM(TM)-ova izvedba protokola IKE (Internet Key Exchange - internetna izmenjava klju─Źev). Upravljalnik klju─Źev podpira samodejno pogajanje glede dogovorov za za┼í─Żito (SA-jev), kot tudi samodejno tvorbo in osve┼żitev ┼íifrirnih klju─Źev.

Dogovor za za┼í─Żito (SA) vsebuje informacije, ki so potrebne za uporabo protokolov IPSec. SA tako na primer dolo─Ża vrste algoritmov, dol┼żine in trajanje klju─Źev, udele┼żene stranke in na─Żine enkapsulacije.

┼áifrirni klju─Źi, kot pove ┼że samo ime, zaklenejo ali ┼í─Żitijo informacije, dokler ne pridejo do kon─Żnega cilja.

Opomba: Za┼í─Żitena tvorba klju─Źev je najpomembnej┼íi faktor pri vzpostavitvi za┼í─Żitene in zasebne povezave. ─îe so klju─Źi stisnjeni, bodo vsi poskusi overjanja in ┼íifriranja, pa naj bodo ┼íe tako mo─Źni, neuspe┼íni.

Faze upravljanja klju─Źev

Upravljalnik klju─Źev VPN uporablja v svoji izvedbi dve lo─Żeni fazi.

Prva faza

Prva faza vzpostavi glavno skrivnost, iz katere izhajajo nadaljnji ┼íifrirni klju─Źi, da za┼í─Żiti promet uporabni┼íkih podatkov. To velja tudi, ─Że med dvema zaklju─Źnima to─Źkama ┼íe ne obstaja za┼í─Żita. VPN overi pogajanja prve faze s pomo─Źjo podpisnega na─Żina RSA ali klju─Źev z vnaprej dolo─Żeno skupno rabo, s katerimi tudi vzpostavi klju─Że, ki ┼í─Żitijo sporo─Żila IKE, ki potujejo med nadaljnjimi pogajanji druge faze.

Klju─Ź z vnaprej dolo─Żeno skupno rabo je nerazviden niz dol┼żine do 128 znakov. Klju─Ź z vnaprej dolo─Żeno skupno rabo morata potrditi oba konca povezave. Prednost uporabe klju─Źev z vnaprej dolo─Żeno skupno rabo je njihova preprostost, slabost pa, da mora biti skupna skrivnost pred pogajanji IKE poslana izven pasu, na primer prek telefona ali registrirane po┼íte. Ta klju─Ź obravnavajte kot geslo.

Overjanje s *podpisom RSA* nudi ve─Źjo za┼í─Żito kot klju─Źi z vnaprej dolo─Żeno skupno rabo, saj ta na─Żin nudi overjanje s pomo─Źjo digitalnih potrdil. Digitalna potrdila morate konfigurirati z Upravljalnikom digitalnih potrdil (mo┼żnost 5722-SS1 34). Nekatere re┼íitve VPN zahtevajo podpis RSA za vzajemno delovanje. Tako na primer uporablja VPN v Windows(R) 2000 podpis RSA kot svoj privzeti na─Żin overjanja. Podpis RSA nudi tudi ve─Źjo skalabilnost kot klju─Źi z vnaprej dolo─Żeno skupno rabo. Potrdila, ki jih uporabite, morajo izdati slu┼żbe za pooblastila, ki jim zaupata oba stre┼żnika klju─Źev.

Druga faza

V drugi fazi potekajo pogajanja glede dogovorov za za┼í─Żito in klju─Źev, ki ┼í─Żitijo dejansko izmenjavo podatkov aplikacij. Ne pozabite, da do zdaj niso bili poslani ┼íe nobeni podatki aplikacije. Prva faza ┼í─Żiti sporo─Żila IKE druge faze.

Ko so pogajanja druge faze kon–Źana, VPN vzpostavi za┼í–Źiteno, dinami–Źno povezavo prek omre┼żja in med zaklju–Źnima to–Źkama, ki ste ju definirali za povezavo. Vsi podatki, ki potujejo prek VPN, so preneseni s stopnjo za┼í–Źite in u–Źinkovitosti, ki jo dogovorita stre┼żnika klju–Źev med postopkom pogajanj prve in druge faze.

Na splo┼íno se odvijajo pogajanja prve faze enkrat dnevno, pogajanja druge faze pa so osve┼żena vsakih 60 minut ali celo vsakih pet minut. Pogostej┼íe osve┼żitve pove–Źajo za┼í–Źito podatkov, toda zmanj┼íajo u–Źinkovitost sistema. Za za┼í–Źito najpomembnej┼íih podatkov uporabite klju–Źe s kratkim trajanjem.

–îe izdelate dinami–Źni VPN s pomo–Źjo Navigatorja iSeries(TM), morate definirati na–Źelo IKE, da omogo–Źite pogajanja prve faze, in podatkovno na–Źelo, ki bo vodilo pogajanja druge faze. –îe ┼żelite, lahko uporabite –Źarovnika Nova povezava. –îarovnik samodejno izdela vse konfiguracijske objekte, ki jih zahteva VPN za pravilno delovanje, kar vklju–Źuje tudi podatkovno na–Źelo.

Predlagano –Źtivo
–îe ┼żelite prebrati ┼íe kaj ve–Ź o protokolu IKE (Internet Key Exchange) in upravljanju klju–Źev, preglejte naslednje RFC-je (Request for Comments) IETF (Internet Engineering Task Force):

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

Te RFC-je si lahko ogledate tudi na naslednji spletni strani: http://www.rfc-editor.org

.

L2TP (Layer 2 Tunnel Protocol)

Povezave L2TP (Layer 2 Tunneling Protocol), imenovane tudi navidezne linije, omogo–Źajo stro┼íkovno ustrezen dostop za oddaljene uporabnike, saj omogo–Źajo, da zdru┼żen stre┼żnik upravlja naslove IP, dodeljene njegovim oddaljenim uporabnikom. Povezave L2TP poleg tega nudijo tudi varen dostop do sistema ali omre┼żja, –Źe jih uporabite skupaj z IPSec (IP Security)

L2TP podpira dva na–Źina tunela: prostovoljen tunel in obvezen tunel. Glavna razlika med tema na–Źinoma tunela je zaklju–Źna to–Źka. V prostovoljnem tunelu se kon–Źa tunel na oddaljenem odjemalcu, obvezen tunel pa pri ISP.

Z **obveznim tunelom** L2TP inicializira oddaljeni gostitelj povezavo s svojim ponudnikom internetnih storitev (ISP-jem). Nato vzpostavi ISP povezavo L2TP med oddaljenim gostiteljem in zdru┼żenim omre┼żjem. –îeprav vzpostavi povezavo ISP, vi odlo–Źite, kako boste za┼í–Źitili promet s pomo–Źjo VPN. –îe uporabite obvezni tunel, mora ISP podpirati LT2P.

V **prostovoljnem tunelu** L2TP izdela povezavo oddaljen uporabnik, in sicer obi–Źajno z uporabo odjemalca tunela L2TP. Posledi–Źno po┼ílje oddaljeni uporabnik pakete L2TP svojemu ISP-ju, ki jih razpo┼ílje v zdru┼żeno omre┼żje. –îe uporabite prostovoljni tunel, ni nujno, da ISP podpira L2TP. Scenarij *Za┼í–Źita prostovoljnega tunela L2TP z IPSec* ka┼że zgled za konfiguriranje povezave iSeries podru┼żnice s zdru┼żenim omre┼żjem prek prehoda iSeries(TM) s tunelom L2TP, ki ga ┼í–Źiti VPN.

Prika┼żete lahko vizualno predstavitev zasnove prostovoljnih tunelov L2TP, ki so za┼í–Źiteni z IPSec. To zahteva dodatek Flash

. Ogledate si lahko tudi razli–Źico HTML te predstavitve.

«

L2TP je dejansko razli─Źica protokola za enkapsulacijo IP. Tunel L2TP je izdelan z enkapsulacijo okvirja L2TP znotraj paketa UDP (User Datagram Protocol), ki je v zameno enkapsuliran znotraj paketa IP. Izvorni in ciljni naslov tega paketa IP definirata zaklju─Źni to─Źki povezave. Ker je zunanji protokol za enkapsuliranje IP, lahko za zdru┼żeni paket IP uporabite protokole IPSec. S tem za┼í─Žitite podatke, ki potujejo znotraj tunela L2TP. Nato lahko na obi─Źajen na─Źin uporabite protokole AH (Authentication Header), ESP (Encapsulated Security Payload) in IKE (Internet Key Exchange).

Scenarij: Konfiguriranje oddaljene klicne povezave PPP nudi zgled uporabe protokola L2TP pri povezovanju z IBM(R)-om prek univerzalne povezave.

Prevod omre┼żnega naslova za VPN

Prevod omre┼żnega naslova (NAT) prevede zasebne naslove IP v javne naslove IP. S tem ohranite pomembne javne naslove, obenem pa tudi omogo─Źite gostiteljem v va┼íem omre┼żju dostop do storitev in oddaljenih gostiteljev prek interneta (ali drugega javnega omre┼żja).

─Źe uporabite zasebne naslove IP, lahko pride do navzkri┼żja s podobnimi vhodnimi naslovi IP. Komunicirati ┼żelite na primer z drugim omre┼żjem, toda obe omre┼żji uporabljata naslova 10.*.*.*, kar povzro─Źi navzkri┼žje med naslovoma in izbris vseh paketov. Uporaba NAT za izhodne naslove se zdi ustrezna re┼íitev za to te┼żavo. Toda ─Źe je promet podatkov za┼í─Žiten z VPN, obi─Źajni NAT ne bo deloval, ker spremeni naslove IP v dogovorih za za┼í─Žito (SA-jih), ki jih zahteva VPN za delovanje. Da bi se izognili tej te┼żavi, nudi VPN lastno razli─Źico prevoda omre┼żnega naslova, imenovano VPN NAT. VPN NAT opravi prevod naslova pred preverjanjem veljavnosti SA, tako da dodeli naslov povezavi pri njenem zagonu. Naslov ostane povezan s povezavo, dokler je ne zbri┼íete.

Opomba: FTP zdaj ne podpira VPN NAT.

Kako naj uporabljam VPN NAT?
Na voljo sta dve razli─Źni vrsti VPN NAT, o katerih morate razmisliti, preden za─Źnete. To sta:

VPN NAT za prepre─Ćevanje navzkri┼żij med naslovi IP
Ta vrsta VPN NAT omogo─Ża, da se izognete mo┼żnim navzkri┼żjem med naslovi IP pri konfiguriranju povezave VPN med omre┼żji ali sistemi s podobnimi shemami naslovov. Zna─Źilen primer sta dve podjetji, ki ┼żelita izdelati povezave VPN s pomo─Źjo enega izmed dolo─Źenih obmo─Źij zasebnih naslovov IP, kot je na primer 10.*.*.*. Kako konfigurirate to vrsto VPN NAT je odvisno od tega, ali je stre┼żnik pobudnik ali odzivnik za povezavo VPN. ─Źe je stre┼żnik pobudnik povezave, lahko prevede lokalne naslove v naslove, ki so zdru┼żljivi z naslovi partnerja v povezavi VPN. ─Źe je stre┼żnik odzivnik povezave, lahko prevedete oddaljene naslove partnerja VPN v naslove, ki so zdru┼żljivi z lokalno shemo naslovov. To vrsto prevoda naslovov konfigurirajte samo za dinami─Źne povezave.

VPN NAT za skritje lokalnih naslovov
Ta vrsta VPN NAT so v glavnem uporablja za skritje realnega naslova IP lokalnega sistema s prevodom v drug naslov, ki je na voljo javno. Ko konfigurirate VPN NAT, lahko podate, naj bo vsak javno znan naslov IP preveden v enega izmed naslovov iz podro─Źja skritih naslovov. To omogo─Ża tudi uravnote┼żenje prometa za posamezen naslov prek ve─Ź naslovov. VPN NAT za lokalne naslove zahteva, da va┼í stre┼żnik deluje kot odzivnik za to povezavo.

VPN NAT uporabite za skritje lokalnih naslovov, ─Źe na naslednja vpra┼íanja odgovorite z da:

1. Ali uporabljate enega ali ve─Ź stre┼żnikov, do katerih bodo uporabniki dostopali s pomo─Źjo VPN?
2. Ali potrebujete pro┼żnost pri dejanskih naslovih IP v sistemih?
3. Ali uporabljate enega ali ve─Ź naslovov IP z mo┼żnostjo globalnega usmerjanja?

V scenariju *Uporaba prevoda omre┼żnega naslova za VPN* boste na┼íli zgled za konfiguracijo VPN NAT za skritje lokalnih naslovov v sistemu iSeries(TM).

Navodila po korakih za nastavitev VPN NAT na iSeries poi┼í─Źite v zaslonski pomo─Źi, ki je na voljo v vmesniku VPN Navigatorja iSeries.

IPSec, zdru┼żljiv z NAT

Te┼żava: obi─Źajni NAT prekine VPN

Prevod omre┼żnega naslova (NAT) omogo─Źa, da skrijete neregistriran zasebni naslov IP za niz registriranih naslovov IP. S tem za┼í─Źitite notranje omre┼że pred zunanjimi omre┼żji. NAT pomaga tudi pri zmanj┼ívanju te┼żav, povezanih z izpraznitvijo naslovov IP, saj je lahko veliko zasebnih naslovov predstavljenih z majhnim nizom registriranih naslovov.

Toda na ┼żalost obi─Źajni NAT ne deluje na pakete IPSec, saj se pri prehodu paketa skozi napravo NAT spremenita izvorni naslov in paket, s ─Źimer se paket razveljavi. V tem primeru sprejemni konec povezave VPN zavrne paket, pogajanja za povezavo VPN pa ne uspejo.

Re┼íitev: enkapsulacija UDP
Na kratko povedano enkapsulacija UDP skrije paket IPSec znotraj novega, toda podvojenega oglavja IP/UDP. Naslov v novem oglavju IP je preveden pri prehodu skozi napravo NAT. Ko pride paket do cilja, sprejemni konec odre┼že dodatno oglavje in pusti izvirni paket IPSec, ki bo zdaj prestal vsa druga preverjanja veljavnosti.

Enkapsulacijo UDP lahko uporabite samo za VPN-je, ki bodo uporabljali IPSec ESP v na─Źinu tunela ali v na─Źinu prenosa. Poleg tega lahko iSeries(TM) v v5r2 deluje samo kot odjemalec za enkapsulacijo UDP. To pomeni, da lahko samo *inicializira* enkapsuliran promet UDP.

Spodnja grafika ka┼że format paketa ESP, enkapsuliranega z UDP, v na─Źinu tunela:

Izvirni datagram IPv4:

Po uveljavitvi IPSec ESP v na─Źinu tunela:

Po uveljavitvi enkapsulacije UDP:

Spodnja grafika ka┼że format paketa ESP, enkapsuliranega z UDP, v na─Źinu prenosa:

Izvirni datagram IPv4:

Po uveljavitvi IPSec ESP v na─Źinu prenosa:

Po uveljavitvi enkapsulacije UDP:

Ko je paket enkapsuliran, ga iSeries po┼ílje partnerju VPN prek vrat UDP 4500. Partnerji VPN ┼że izvedejo pogajanja IKE prek vrat UDP 500. ─îe IKE odkrije NAT med pogajanjem za klju─Ź, so naslednji paketi IKE poslani prek izvornih vrat 4500 na ciljna vrata 4500. To pomeni tudi, da vrata 4500 ne smejo biti omejena v nobenih ustreznih pravilih za filtriranje. Sprejemni konec povezave lahko dolo─Źi, ali gre za paket IKE ali paket, enkapsuliran z UDP, ker je prvih 4 bajtov tovora UDP v paketu IKE nastavljenih na ni─Ź. ─îe ┼želite, da bo enkapsulacija UDP pravilno delovala, jo morata podpirati oba konca povezave.

Stiskanje IP (IPComp)

Protokol IPComp (IP Payload Compression) s pomo─Źjo stiskanja zmanj┼ía velikost datagramov IP, in tako pove─Ża komunikacijsko zmogljivost med dvema partnerjema. Namen je pove─Żati celotno komunikacijsko zmogljivost, ─Że potekajo komunikacije prek po─Żasnih linij ali linij z zastoji. IPComp ne nudi nobene za┼í─Żite in ga morate pri komuniciranju prek povezave VPN uporabiti skupaj s pretvorbo AH ali ESP.

IETF (Internet Engineering Task Force) formalno definira IPComp v RFC-ju (Request for Comments) 2393, *IP Payload compression Protocol (IPComp)*. RFC si lahko ogledate na internetu na naslednji spletni strani: http://www.rfc-editor.org

.

VPN in filtriranje IP

Ve─Źina povezav VPN zahteva za pravilno delovanje pravila za filtriranje. Zahtevana pravila za filtriranje so odvisna od vrste povezave VPN, ki jo konfigurirate, in od vrste prometa, ki ga ┼želite nadzorovati. Na splo┼íno bo imela vsaka povezava filter na─Źel. Filter na─Źel definira, kateri naslovi, protokoli in vrata lahko uporabljajo VPN. Poleg tega imajo povezave, ki podpirajo protokol IKE (Internet Key Exchange), pogosto pravila, ki so napisana, da izrecno dopu┼í─Żajo obdelavo IKE prek povezave.

Od izdaje operacijskega sistema V5R1 naprej lahko VPN ustvari ta pravila samodejno. ─îe je le mogo─Że, pustite, da VPN za vas izdela filtre na─Źel. S tem ne boste le odpravili napak, pa─Ź pa vam tudi ne bo treba konfigurirati pravil kot lo─Ženega koraka v urejevalniku pravil paketov Navigatorja iSeries(TM).

Seveda obstajajo tudi izjeme. Preberite naslednje teme in spoznajte druge, manj pogoste koncepte in tehnike VPN in filtriranja, ki bodo morda primerni za va┼ío situacijo:

- **Selitev filtrov na─Źel v trenutno izdajo**
  V izdajah operacijskega sistema V4R4 in V4R5 ste morali konfigurirati pravila paketov VPN kot lo─Żen korak. Pravila niso bila izdelana samodejno kot del konfiguriranja VPN. Tema podrobno razlaga posebno problematiko selitve filtrov na─Źel V4R4 in V4R5 v trenutno izdajo in opi┼íe, kako opraviti ta postopek.
- **Povezava VPN brez filtrov na─Źel**
  ─îe so zaklju─Źne to─Źke povezave VPN samostojni, specifi─Źni naslovi IP, in ┼želite zagnati VPN, ne da bi morali v sistemu napisati ali aktivirati pravila za filtriranje, lahko konfigurirate dinami─Żen filter na─Źel. Tema razlaga, zakaj bi se odlo─Żili za to mo┼żnost in kako jo izvesti.
- **Implicitni IKE**
  ─îe ┼želite, da bodo za VPN izvedena pogajanja IKE, morate omogo─Żiti datagrame UDP prek vrat 500 za to vrsto

prometa IP. Toda –Źe v sistemu ni nobenih pravil za filtriranje, ki bi izrecno dovoljevala promet IKE, bo sistem implicitno omogo–Źil tok prometa IKE. V tej temi boste na┼íli podrobnej┼íe informacije o tem, kako to deluje na iSeries.

Selitev filtrov na–Źel v trenutno izdajo

V izdajah operacijskega sistema V4R4 in V4R5 ste morali konfigurirati pravila paketov VPN kot lo–Źen korak v vmesniku pravil paketov Navigatorja iSeries(TM). Pravila niso bila izdelana samodejno kot del konfiguriranja VPN. Od izdaje operacijskega sistema V5R1 naprej lahko VPN GUI ta pravila paketov izdela samodejno.

V V4R4 in V4R5 ste morali pri izdelavi pravil za filtriranje na–Źel (pravila, kjer je dejanje=IPSEC) upo┼ítevati ┼ítevilne postavke, in zdaj ┼żelite ta ista pravila uporabiti v trenutni izdaji. Ali pa *bo* pravila za filtriranje na–Źel za vas morda izdelal VPN, toda dodati morate dodatna pravila, ki bodo prek povezave omogo–Źala drug promet IP, kot je na primer telnet. Naslednja priporo–Źila vam bodo pomagala, da se boste izognili mo┼żnim napakam v konfiguraciji.

Pojasnilo: –îe v tej temi govorimo o datoteki pravil *uporabnika*, to pomeni katerokoli datoteko pravil, ki ste jo izdelali s pomo–Źjo urejevalnika pravil paketov v Navigatorju iSeries. Primerjajte z datoteko pravil *VPNPOLICYFILTERS.I3P*, ki jo VPN samodejno izdela kot del konfiguriranja VPN.

- –îe imate povezave VPN iz V4R4 ali V4R5 in v trenutni izdaji ne nameravate konfigurirati drugih povezav VPN, lahko po obi–Źajnem postopku aktivirate pravila za filtriranje in za┼żenete povezave.
- –îe imate povezave VPN iz V4R4 ali V4R5 in nameravate v trenutni izdaji izdelati nove povezave VPN, uporabite –Źarovnika **Selitev filtrov na–Źel**. –îarovnik odstrani filtre na–Źel iz datotek s pravili paketov, ki ste jih izdelali, in vstavi enakovredne filtre na–Źel v VPNPOLICYFILTERS.I3P, ki jo ustvari VPN. Do –Źarovnika dostopite takole:
  1. V Navigatorju iSeries raz┼íirite ikono stre┼żnika —**>Omre┼żje** —**>Na–Źela IP**.
  2. Z desno tipko mi┼íke kliknite **Delo z navideznim zasebnim omre┼żjem** in izberite **Selitev filtrov na–Źel**.
  3. Ko izpolnite –Źarovnika, kliknite **Dokon–Źaj**.
  4. –îe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo–Ź**.
- –îe je pravila za filtriranje na–Źel ustvaril VPN, toda dodati morate ┼íe nekaj pravil za filtriranje, ki niso VPN, jih morate konfigurirati s pomo–Źjo urejevalnika pravil paketov v Navigatorju iSeries. –îe morajo ta pravila za filtriranje, ki niso VPN, priti pred filtre VPN, za–Źnite njihova imena z PREIPSEC, na primer PREIPSECMYRULES. Na ta na–Źin sistemu pomagate pri dolo–Źitvi vrstnega reda za obdelavo pravil za filtriranje. Imena nizov za pravila, ki niso VPN, ne smejo imeti predpone PREIPSEC. Na primer MORERULES.
- Vedno omogo–Źite VPN-ju, da izdela pravila za filtriranje na–Źel. Toda pravila za filtriranje na–Źel, ki niso VPN, morajo ostati v datoteki pravil uporabnika. Ne mora katerikoli izmed teh filtrov, ki niso VPN, priti pred filtre na–Źel v datoteki pravil VPNPOLICYFILTERS.I3P, morate pred ime niza dodati PREIPSEC. S tem boste zagotovili, da bodo pravila uporabnika in pravila VPN skupaj delovala tako kot ste na–Źrtovali. Denimo, da je VPN ustvaril va┼ía pravila za filtriranje na–Źel (nizi VPN), vi pa ste dodali dodatna pravila (Va┼íi nizi), ki bodo omogo–Źila promet IP prek povezave. Ko nalo┼żite pravila v sistem, bo njihov vrstni red tak┼íen:
  1. Va┼íi nizi, katerih imena se za–Źno s PREIPSEC
  2. Nizi VPN, katerih imena se za–Źno s PREIPSEC
  3. Nizi VPN z ACTION=IPSEC (filtri na–Źel)
  4. Va┼íi nizi z ACTION=IPSEC (filtri na–Źel)
  5. Va┼íi nizi s –Źimerkoli drugim.
  6. Nizi VPN s –Źimerkoli drugim.

  V datoteki EXPANDED.OUT si oglejte vrstni red v zdru┼żeni izhodni datoteki. Datoteka EXPANDED.OUT je zapisana v imenik, v katerem je shranjena datoteka s pravili uporabnika.
- S pomo–Źjo Navigatorja iSeries lahko aktivirate naslednje:
  – samo datoteko pravil, ki jo je ustvaril VPN, imenovano VPNPOLICYFILTERS.I3P
  – samo va┼ío datoteko s pravili uporabnika
  – datoteko s pravili, ki jih je ustvaril VPN in va┼ío datoteko s pravili uporabnika
- Pravila za filtriranje aktivirajte za vse vmesnike in ne za posamezne vmesnike. S tem boste zagotovili aktiviranje filtrov in nastavili pravilen vrstni red filtrov na–Źel.

- Preden aktivirate pravila za filtriranje, jih vedno preverite. –ie ni pri preverjanju pri┼ílo do nobene napake, preverite ┼íe EXPANDED.OUT in zagotovite, ali so pravila navedena v ┼želenem vrstnem redu. Ko kon–Źate ta korak, lahko aktivirate pravila.

Povezave VPN brez filtrov na–Źel

Pravilo za filtriranje na–Źel definira, kateri naslovi, protokoli in vrata lahko uporabljajo VPN, in usmerja ustrezen promet prek povezave. V–Źasih boste ┼želeli konfigurirati povezavo, ki ne zahteva pravila za filtriranje na–Źel. Morda imate v vmesnik, ki ga bo uporabljala povezava VPN, nalo┼żena pravila paketov, ki niso VPN, in namesto, da bi deaktivirali aktivna pravila, se odlo–Żite, da boste konfigurirali VPN, tako da bo sistem vse filtre za povezavo upravljal dinami–Źno. Filter na–Źel za to vrsto povezave se imenuje **dinami–Źen filter na–Źel**. Preden lahko za povezavo VPN uporabite dinami–Źen filter na–Źel, mora veljati vse od naslednjega:

- Povezavo lahko inicializira samo lokalni stre┼żnik
- Podatkovne zaklju–Źne to–Źke povezave morajo biti samostojni sistemi, kar pomeni, da niso podmre┼ża ali obmo–Źje naslovov.
- Za povezavo ni mogo–Źe nalo┼żiti nobenega pravila za filtriranje na–Źel.

–ie va┼ía povezava ustreza tem kriterijem, jo lahko konfigurirate tako, da ne bo zahtevala filtra na–Źel. Ko se povezava za┼żene, bo promet med podatkovnimi zaklju–Źnimi to–Źkami potoval prek nje ne glede na druga pravila paketov, ki so nalo┼żena v sistem.

Navodila po korakih za konfiguriranje povezave, tako da ne bo zahtevala filtra na–Źel, poi┼í–Żite v zaslonski pomo–Źi za VPN.

Implicitni IKE

Za vzpostavitev povezave zahteva ve–Źina VPN-jev, da se pogajanja IKE (izmenjava internetnega klju–Ża) odvijejo, preden se lahko spro┼żi obdelava IPSec. IKE uporablja znana vrata 500, zato morate za pravilno delovanje IKE omogo–Źiti datagrame UDP prek vrat 500 za to vrsto prometa IP. –ie v sistemu ne obstajajo nobena pravila za filtriranje, ki bi izrecno dovoljevala promet IKE, je le-ta implicitno dovoljen. Toda pravila, napisana posebej za vrata UDP 500, so obravnavana na osnovi zapisa, definiranega v aktivnih pravilih za filtriranje.

Na–Źrtovanje za VPN

Na–Źrtovanje je bistven del celotne re┼íitve VPN. Za zagotovitev pravilnega delovanja povezave morate opraviti precej zapletenih odlo–Żitev. S pomo–Źjo naslednjih virov zberite vse informacije, potrebne za uspe┼íno delovanje VPN:

- **Zahteve za nastavitev VPN**
  Preden za–Źnete, preverite, ali zadovoljujete minimalne zahteve za izdelavo VPN.
- **Dolo–Żitev, katero vrsto VPN izdelati**
  Dolo–Żitev, kako boste uporabljali VPN, je eden izmed prvih korakov uspe┼ínega na–Źrtovanja. Tema opisuje razli–Źne vrste povezav, ki jih lahko konfigurirate.
- **Uporaba svetovalca za na–Źrtovanje VPN**
  Svetovalec za na–Źrtovanje vam bo postavil vpra┼íanja o va┼íem omre┼żju in na osnovi va┼íih odgovorov podal predloge za izdelavo VPN.
  Opomba: Svetovalca za na–Źrtovanje VPN uporabite samo za povezave, ki podpirajo protokol IKE (Internet Key Exchange). Za ro–Źne povezave uporabite na–Źrtovalno preglednico.
- **Izpolnitev na–Źrtovalnih preglednic VPN**
  –ie ┼żelite, lahko natisnete na–Źrtovalne preglednice in jih izpolnite kot pomo–Ź pri zbiranju podrobnih informacij za na–Źrtovanje VPN.

Ko izdelate na–Źrt za VPN, lahko za–Źnete s konfiguriranjem.

Zahteve za nastavitev VPN

–ie ┼żelite, da bo VPN pravilno deloval na iSeries(TM) in na omre┼żnih odjemalcih, morata iSeries in odjemalec PC ustrezati naslednjim zahtevam:

Zahteve za iSeries V5R2

- OS/400(R) razli–Źice 5, izdaje 2 (5722-SS1) ali novej┼íe
- Upravljalnik digitalnih potrdil (mo┼żnost 5722-SS1 34)
- Ponudnik ┼íifriranega dostopa (5722-AC2 ali AC3)
- iSeries Access za Windows(R)(5722-XE1) in Navigator iSeries
  - Omre┼żna komponenta Navigatorja iSeries
- Nastavite sistemsko vrednost za ohranitev za┼í–Źitnih podatkov stre┼żnika (QRETSVRSEC *SEC) na 1
- Konfigurirati morate TCP/IP, vklju–Źno z vmesniki IP, smermi, imenom lokalnega gostitelja in imenom lokalne domene

Zahteve za odjemalca

- Delovna postaja z name┼í–Ženim 32-bitnim operacijskim sistemom Windows(R), pravilno povezana z iSeries in konfigurirana za TCP/IP
- 233 Mhz procesorska enota
- 32 MB RAM za odjemalce Windows 95/98
- 64 MB RAM za odjemalce Windows NT(R) in 2000
- Name┼í–Žena iSeries Access za Windows in Navigator iSeries na PC-ju odjemalca
- Programska oprema, ki podpira protokol IPSec (IP Security)
- Programska oprema, ki podpira L2TP, –Źe bodo oddaljeni uporabniki vzpostavljali povezavo z va┼íim sistemom s pomo–Źjo L2TP

Dolo–Žitev, katero vrsto VPN izdelati

Dolo–Žitev, kako boste uporabljali VPN, je eden izmed prvih korakov uspe┼ínega na–Źrtovanja. Najprej morate razumeti vlogo, ki jo imata lokalni stre┼żnik klju–Žev in oddaljeni stre┼żnik klju–Žev v povezavi. Ali se na primer zaklju–Žne to–Žke *povezave* razlikujejo od *podatkovnih* zaklju–Žnih to–Žk? Ali so enake ali pa so kombinacija obeh? Zaklju–Žne to–Žke povezave overjajo in ┼íifrirajo (ali de┼íifrirajo) promet podatkov za povezavo in po izbiri omogo–Žajo tudi upravljanje klju–Žev s protokolom IKE (Internet Key Exchange). Podatkovne zaklju–Žne to–Žke pa definirajo povezavo med dvema sistemoma za promet IP, ki potuje prek VPN - na primer ves promet TCP/IP med 123.4.5.6 in 123.7.8.9. –če se zaklju–Žne to–Žke povezave in podatkov razlikujejo, je stre┼żnik VPN prehod, –Źe pa so iste, je stre┼żnik VPN gostitelj.

Sledijo razli–Žne vrste izvedb VPN, ki so primerne za ve–Žino poslovnih potreb:

Od prehoda do prehoda
Zaklju–Žne to–Žke povezave obeh sistemov se razlikujejo od podatkovnih zaklju–Žnih to–Žk. Protokol IPSec (IP Security) ┼í–Žiti promet na njegovi poti med prehodi. Toda IPSec ne ┼í–Žiti prometa podatkov na eni ali drugi strani prehodov znotraj notranjih omre┼żij. To je obi–Žajna nastavitev povezav med podru┼żnicami, ker je promet, ki je usmerjen izven prehodov podru┼żnice v notranja omre┼żja, pogosto smatran za overjenega.

Od prehoda do gostitelja
IPSec ┼í–Žiti promet podatkov na njegovi poti med prehodom in gostiteljem v oddaljenem omre┼żju. VPN ne ┼í–Žiti prometa podatkov v lokalnem omre┼żju, ker menite, da je overjen.

Od gostitelja do prehoda
VPN ┼í–Žiti promet podatkov na njegovi poti med gostiteljem v lokalnem omre┼żju in oddaljenim prehodom. VPN ne ┼í–Žiti prometa podatkov v oddaljenem omre┼żju.

Od gostitelja do gostitelja
Zaklju–Žne to–Žke povezave so iste kot podatkovne zaklju–Žne to–Žke v lokalnem in oddaljenem sistemu. VPN ┼í–Žiti promet podatkov na njegovi poti med gostiteljem v lokalnem omre┼żju in gostiteljem v oddaljenem omre┼żju. Ta vrsta VPN nudi za┼í–Žito IPSec od enega konca do drugega.

Izpolnitev na–Źrtovalnih preglednic VPN

S pomo–Źjo na–Źrtovalnih preglednic VPN zberite podrobne informacije o na–Źrtih za uporabo VPN. Te informacije boste potrebovali za ustrezno na–Źrtovanje strategije VPN, lahko pa jih uporabite tudi za konfiguriranje VPN. Izberite preglednico za vrsto povezave, ki jo ┼żelite izdelati.

- **Na–Źrtovalna preglednica za dinami–Źne povezave**
  To preglednico izpolnite, preden konfigurirate dinami–Źno povezavo.
- **Na–Źrtovalna preglednica za ro–Źne povezave**
  To preglednico izpolnite, preden konfigurirate ro–Źno povezavo.
- **Svetovalec za na–Źrtovanje VPN**
  Uporabite lahko tudi svetovalca za interaktivno vodenje pri na–Źrtovanju in konfiguriranju. Svetovalec za na–Źrtovanje vam bo postavil vpra┼íanja o va┼íem omre┼żju in na osnovi va┼íih odgovorov podal predloge za izdelavo VPN.

  Opomba: Svetovalca za VPN uporabite samo za dinami–Źne povezave. Za ro–Źne povezave uporabite na–Źrtovalno preglednico.

–îe boste izdelali ve–Ź povezav s podobnimi lastnostmi, lahko nastavite privzete vrednosti VPN. Privzete vrednosti, ki jih nastavite, izpolnijo strani lastnosti VPN. To pomeni, da vam istih lastnosti ni potrebno ve–Źkrat konfigurirati. Za nastavitev privzetih vrednosti VPN izberite z glavnega menija VPN **Urejanje**, nato pa **Privzetki**.

Na–Źrtovalna preglednica za dinami–Źne povezave

Preden izdelate dinami–Źne povezave VPN, izpolnite to preglednico. Preglednica je izdelana na predpostavki, da boste uporabili –Źarovnika Nova povezava. –îarovnik omogo–Źa, da nastavite VPN na podlagi osnovnih zahtev za za┼í–Źito. V–Źasih bo potrebno izbolj┼íati lastnosti, ki jih konfigurira –Źarovnik za povezavo. Tako se lahko na primer odlo–Źite, da potrebujete bele┼żenje ali da ┼żelite, da se stre┼żnik VPN za┼żene pri vsakem zagonu TCP/IP. V tem primeru z desno tipko mi┼íke kliknite skupino dinami–Źnih klju–Źev ali povezavo, ki jo je izdelal –Źarovnik, in izberite **Lastnosti**.

Preden nadaljujete z nastavitvijo VPN, odgovorite na vsa vpra┼íanja.

Potrditveni seznam za zahtevano programsko opremo	Odgovori
Ali uporabljate OS/400(R) izdaje V5R2 (5722-SS1) ali novej┼íe?	
Ali ste namestili Upravljalnik digitalnih potrdil (mo┼żnost 5722-SS1 34)?	
Ali ste namestili ponudnik ┼íifriranega dostopa (5722-AC2 ali AC3)?	
Ali ste namestili iSeries(TM) Access(5722-XE1)?	
Ali ste namestili Navigator iSeries?	
Ali ste namestili omre┼żno podkomponento Navigatorja iSeries?	
Ali ste namestili pomo┼żne programe TCP/IP za povezljivost za OS/400 (5722-TC1)?	
Ali ste nastavili sistemsko vrednost za ohranitev za┼í–Źitnih podatkov stre┼żnika (QRETSVRSEC *SEC) na 1?	
Ali je na iSeries konfiguriran TCP/IP (vklju–Źno z vmesniki IP, smermi, imenom lokalnega gostitelja in imenom lokalne domene)?	
Ali je med zahtevanima zaklju–Źnima to–Źkama vzpostavljeno obi–Źajno komuniciranje TCP/IP?	
Ali ste uveljavili najnovej┼íe za–Źasne popravke programa (PTF-je)?	
Ali pravila za filtriranje po┼żarnega zidu ali usmerjevalnika podpirajo protokola AH in ESP, –Źe pre–Źka tunel VPN po┼żarne zidove ali usmerjevalnike, ki uporabljajo pravila za filtriranje paketov IP?	
Ali so po┼żarni zidovi in usmerjevalniki konfigurirani tako, da dopu┼í–Źajo protokole IKE (UDP vrata 500), AH in ESP?	
Ali so po┼żarni zidovi konfigurirani tako, da omogo–Źajo odpo┼íiljanje IP?	

Te informacije potrebujete za konfiguriranje dinami–Źne povezave VPN	Odgovori
Kak┼íno vrsto povezave izdelujete? • Od prehoda do prehoda • Od gostitelja do prehoda • Od prehoda do gostitelja • Od gostitelja do gostitelja	
Kako boste poimenovali skupino dinami–Źnih klju–Źev?	
Kak┼íno vrsto za┼í–Źite in zmogljivosti sistema potrebujete za za┼í–Źito klju–Źev? • Najvi┼íja za┼í–Źita, najni┼żja zmogljivost • Uravnote┼żena za┼í–Źita in zmogljivost • Najni┼żja za┼í–Źita in najvi┼íja zmogljivost	
Ali overjate povezavo s pomo–Źjo potrdil? –îe ne, kak┼íen je klju–Ź z vnaprej dolo–Źeno skupno rabo?	
Kak┼íen je identifikator lokalnega stre┼żnika klju–Źev?	
Kak┼íen je identifikator lokalne podatkovne zaklju–Źne to–Źke?	
Kak┼íen je identifikator oddaljenega stre┼żnika klju–Źev?	
Kak┼íen je identifikator oddaljene podatkovne zaklju–Źne to–Źke?	
Kak┼íno vrsto za┼í–Źite in zmogljivosti sistema potrebujete za za┼í–Źito podatkov? • Najvi┼íja za┼í–Źita, najni┼żja zmogljivost • Uravnote┼żena za┼í–Źita in zmogljivost • Najni┼żja za┼í–Źita in najvi┼íja zmogljivost	

Na–Źrtovalna preglednica za ro–Źne povezave

Izpolnite to preglednico, ki vam bo pomagala pri izdelavi povezav navideznega zasebnega omre┼żja (VPN), ki za upravljanje klju–Źev ne uporabljajo IKE.

Preden za–Źnete z nastavitvijo VPN, odgovorite na vsa vpra┼íanja:

Predpogojni potrditveni seznam	Odgovori
Ali uporabljate OS/400(R) izdaje V5R2 (5722-SS1) ali novej┼íe?	
Ali ste namestili Upravljalnik digitalnih potrdil (mo┼żnost 5722-SS1 34)?	
Ali ste namestili ponudnik ┼íifriranega dostopa (5722-AC2 ali AC3)?	
Ali ste namestili iSeries(TM) Access(5722-XE1)?	
Ali ste namestili Navigator iSeries?	
Ali ste namestili omre┼żno podkomponento Navigatorja iSeries?	
Ali ste namestili pomo┼żne programe TCP/IP za povezljivost za OS/400 (5722-TC1)?	
Ali ste nastavili sistemsko vrednost za ohranitev za┼í–Źitnih podatkov stre┼żnika (QRETSVRSEC *SEC) na 1?	
Ali je na iSeries konfiguriran TCP/IP (vklju–Źno z vmesniki IP, smermi, imenom lokalnega gostitelja in imenom lokalne domene)?	
Ali je med zahtevanima zaklju–Źnima to–Źkama vzpostavljeno obi–Źajno komuniciranje TCP/IP?	
Ali ste uveljavili najnovej┼íe za–Źasne popravke programa (PTF-je)?	
Ali pravila za filtriranje po┼żarnega zidu ali usmerjevalnika podpirajo protokola AH in ESP, –Źe pre–Źka tunel VPN po┼żarne zidove ali usmerjevalnike, ki uporabljajo pravila za filtriranje paketov IP?	

Predpogojni potrditveni seznam	Odgovori
Ali so po┼žarni zidovi in usmerjevalniki konfigurirani tako, da dopu┼í─Żajo protokole AH in ESP?	
Ali so po┼žarni zidovi konfigurirani tako, da omogo─Żajo odpo┼íiljanje IP?	

Te informacije boste potrebovali za konfiguriranje ro─Żne povezave VPN	Odgovori
Kak┼íno vrsto povezave izdelujete? • Od gostitelja do gostitelja • Od gostitelja do prehoda • Od prehoda do gostitelja • Od prehoda do prehoda	
Kako boste poimenovali povezavo?	
Kak┼íen je identifikator lokalne zaklju─Żne to─Żke povezave?	
Kak┼íen je identifikator oddaljene zaklju─Żne to─Żke povezave?	
Kak┼íen je identifikator lokalne podatkovne zaklju─Żne to─Żke?	
Kak┼íen je identifikator oddaljene podatkovne zaklju─Żne to─Żke?	
Katero vrsto prometa boste omogo─Żili za to povezavo (lokalna vrata, oddaljena vrata in protokol)?	
Ali potrebujete za to povezavo prevod naslova? Podrobnej┼íe informacije poi┼í─Żite v Prevod omre┼żnega naslova za VPN.	
Ali boste uporabili na─Żin tunela ali na─Żin prenosa?	
Kateri protokol IPSec bo uporabljala povezava (AH, ESP ali AH z ESP)? Za podrobnej┼íe informacije preglejte IPSec (IP Security).	
Kateri algoritem ┼íifriranja bo uporabljala povezava (HMAC-MD5 ali HMAC-SHA)?	
Kateri algoritem ┼íifriranja bo uporabljala povezava (DES-CBC ali 3DES-CBC)? **Opomba:** Algoritem ┼íifriranja podate samo, ─Że ste kot protokol IPSec izbrali ESP.	
Kak┼íen je vhodni klju─Ż AH? ─îe uporabite MD5, je klju─Ż 16-bajtni ┼íestnajsti┼íki niz. ─îe uporabite SHA, je klju─Ż 20-bajtni ┼íestnajsti┼íki niz. Vhodni klju─Ż se mora natan─Żno ujemati z izhodnim klju─Żem oddaljenega stre┼żnika.	
Kak┼íen je izhodni klju─Ż AH? ─îe uporabite MD5, je klju─Ż 16-bajtni ┼íestnajsti┼íki niz. ─îe uporabite SHA, je klju─Ż 20-bajtni ┼íestnajsti┼íki niz. Izhodni klju─Ż se mora natan─Żno ujemati z vhodnim klju─Żem oddaljenega stre┼żnika.	
Kak┼íen je vhodni klju─Ż ESP? ─îe uporabite DES, je klju─Ż 8-bajtni ┼íestnajsti┼íki niz. ─îe uporabite 3DES, je klju─Ż 24-bajtni ┼íestnajsti┼íki niz. Vhodni klju─Ż se mora natan─Żno ujemati z izhodnim klju─Żem oddaljenega stre┼żnika.	
Kak┼íen je izhodni klju─Ż ESP? ─îe uporabite DES, je klju─Ż 8-bajtni ┼íestnajsti┼íki niz. ─îe uporabite 3DES, je klju─Ż 24-bajtni ┼íestnajsti┼íki niz. Izhodni klju─Ż se mora natan─Żno ujemati z vhodnim klju─Żem oddaljenega stre┼żnika.	
Kak┼íen je vhodni SPI (Security Policy Index)? Vhodni SPI je 4-bajtni ┼íestnajsti┼íki niz, katerega prvi bajt nastavljen na 00. Vhodni SPI se mora natan─Żno ujemati z izhodnim SPI oddaljenega stre┼żnika.	
Kak┼íen je izhodni SPI? Izhodni SPI je 4-bajtni ┼íestnajsti┼íki niz. Izhodni SPI se mora natan─Żno ujemati z vhodnim SPI oddaljenega stre┼żnika.	

Konfiguriranje VPN

Vmesnik VPN nudi ┼ítevilne razli─Źne na─Źine za konfiguriranje povezav VPN. Nadaljujte z branjem in se odlo─Źite, katero vrsto povezave boste konfigurirali in kako.

Katero vrsto povezave naj konfiguriram?
Dinami─Źna povezava je tista, ki v ─Źasu aktivnosti dinami─Źno ustvarja in dogovarja klju─Że, ki ┼í─Žitijo povezavo, za kar uporablja IKE (Internet Key Exchange). Dinami─Źne povezave nudijo dodatno raven za┼í─Žite za podatke, saj se klju─Źi samodejno spreminjajo v rednih intervalih. Zato ima napadalec manj mo┼żnosti, da bi zajel klju─Ź, imel dovolj ─Źasa da bi ga de┼íifriral in ga uporabil za odvrnitev ali zajetje prometa, ki ga ┼í─Žiti klju─Ź.

Ro─Źna (stran 36) povezava ne nudi podpore za pogajanja IKE in posledi─Źno za samodejno upravljanje klju─Źev. Poleg tega zahtevata oba konca povezave, da konfigurirate ve─Ź atributov, ki se morajo natan─Źno ujemati. Ro─Źne povezave uporabljajo stati─Źne klju─Że, ki se v ─Źasu aktivnosti povezave ne osve┼żijo ali spremenijo. Ro─Źno povezavo morate zaustaviti, ─Że ┼żelite spremeniti z njo povezan klju─Ź. ─Źe menite, da to lahko povzro─Źi tveganje v za┼í─Žiti, je morda bolje, da uporabite dinami─Źno povezavo.

Kako konfiguriram dinami─Źno povezavo VPN?
VPN je dejansko skupina konfiguracijskih objektov, ki definirajo zna─Žilnosti povezave. Dinami─Źna povezava VPN zahteva pravilno delovanje vseh teh objektov. Spodnje povezave podajajo specifi─Źne informacije o konfiguriranju posameznih konfiguracijskih objektov VPN:

> **Nasvet:**
> **Konfiguriranje povezave s pomo─Źjo ─Źarovnika Nova povezava**
> Na splo┼íno priporo─Źamo, da izdelate vse dinami─Źne povezave s pomo─Źjo ─Źarovnika za povezave. ─Źarovnik samodejno izdela vse konfiguracijske objekte, ki jih zahteva VPN za pravilno delovanje, kar vklju─Źuje tudi pravila paketov. ─Źe podate, naj ─Źarovnik za vas aktivira pravila paketov VPN, lahko sko─Źite na ┼ísti korak spodaj *Zagon povezave*. Sicer morate za tem, ko ─Źarovnik kon─Źa s konfiguriranjem VPN, aktivirati pravila paketov in nato zagnati povezavo.

─Źe se odlo─Źite, da za konfiguriranje dinami─Źnih povezav VPN ne boste uporabili ─Źarovnika, dokon─Źajte konfiguriranje s pomo─Źjo naslednjih korakov:

1. **Konfiguriranje na─Źel za┼í─Žite VPN**
   Na─Źela za┼í─Žite VPN morate definirati za vse dinami─Źne povezave. Na─Źelo IKE (Internet Key Exchange) in podatkovno na─Źelo dolo─Żata, kako IKE ┼í─Žiti svojo prvo in drugo fazo pogajanj.
2. **Konfiguriranje za┼í─Žitenih povezav**
   Ko definirate na─Źela za┼í─Žite za povezavo, morate konfigurirati za┼í─Žiteno povezavo. Za dinami─Źne povezave vklju─Źuje za┼í─Žiten povezovalni objekt skupino dinami─Źnih klju─Źev in povezavo prek dinami─Źnega klju─Źa. **Skupina dinami─Źnih klju─Źev** definira splo┼íne zna─Žilnosti ene ali ve─Ź povezav VPN, **povezava prek dinami─Źnega klju─Źa** pa definira zna─Žilnosti posameznih podatkovnih povezav med pari zaklju─Źnih to─Źk. Povezava prek dinami─Źnega klju─Źa obstaja znotraj skupine dinami─Źnih klju─Źev.

   Opomba: Naslednja koraka - *Konfiguriranje pravil paketov* in *Definiranje vmesnika za pravila* - dokon─Źajte samo, ─Że izberete na strani **Skupina dinami─Źnih klju─Źev - Povezave** vmesnika VPN mo┼żnost **Pravilo za filtriranje na─Źel bo definirano v pravilih paketov**. V nasprotnem primeru bodo ta pravila izdelana kot del konfiguracij VPN in bodo uveljavljena za vmesnik, ki ga podate.

   Priporo─Źamo, da vedno dovolite, da vmesnik VPN za vas izdela pravila za filtriranje na─Źel. To naredite tako, da na strani **Skupina dinami─Źnih klju─Źev - Povezave** izberete mo┼żnost **Za to skupino ustvari naslednji filter na─Źel**.
3. **Konfiguriranje pravil paketov**
   Ko kon─Źate konfiguriranje VPN, morate izdelati in uveljaviti pravila za filtriranje, ki omogo─Źajo promet podatkov prek povezave. Pravila VPN **pred-IPSec** dovoljujejo ves promet IKE na podanih vmesnikih, tako da IKE lahko dogovori povezave. Pravilo **filtriranje na─Źel** definira, kateri naslovi, protokoli in vrata lahko uporabijo novo povezano skupino dinami─Źnih klju─Źev.

–îe izvajate selitev iz V4R4 ali V4R5 in ┼želite nadaljevati z uporabo povezav VPN in filtrov na–Źel v trenutni izdaji, preberite temo *Selitev filtrov na–Źel v trenutno izdajo*, in zagotovite, da bodo stari filtri na–Źel in novi filtri na–Źel delovali kot ste nameravali.

4. **Definiranje vmesnika za pravila**
   Ko konfigurirate pravila paketov in vsa druga pravila, ki jih potrebujete, da omogo–Źite povezavo VPN, morate definirati vmesnik, za katerega jih boste uveljavili.
5. **Aktiviranje pravil paketov**
   Ko definirate vmesnik za pravila paketov, jih morate aktivirati, preden za┼ženete povezavo.
6. **Zagon povezave**
   To nalogo dokon–Źajte za zagon povezav.

Kako konfiguriram ro–Źno povezavo VPN?
Kot pove samo ime, je ro–Źna povezava tista, za katero morate konfigurirati vse lastnosti VPN ro–Źno, vklju–Źno z vhodnimi in izhodnimi klju–Źi. Spodnje povezave podajajo specifi–Źne informacije za konfiguriranje ro–Źne povezave:

1. **Konfiguriranje ro–Źnih povezav**
   Ro–Źne povezave definirajo zna–Žilnosti povezave, vklju–Źno z za┼í–Žitnimi protokoli, zaklju–Źno to–Źko povezave in podatkovno zaklju–Źno to–Źko.

   Opomba: Naslednja dva koraka - *Konfiguriranje pravil za filtriranje na–Źel* in *Definiranje vmesnika za pravila* - opravite samo, –Źe na strani **Ro–Źna povezava - Povezava** vmesnika VPN izberete mo┼žnost **Pravilo za filtriranje na–Źel bo definirano v pravilih paketov**. V nasprotnem primeru bodo pravila izdelana kot del konfiguracij VPN.

   Priporo–Žamo, da vedno dovolite, da vmesnik VPN za vas izdela pravila za filtriranje na–Źel. To naredite tako, da na strani **Ro–Źna povezava - Povezava** izberete mo┼žnost **Ustvari filter na–Źel, ki se ujema s podatkovnimi zaklju–Źnimi to–Źkami**.
2. **Konfiguriranje pravila za filtriranje na–Źel**
   Ko konfigurirate atribute ro–Źne povezave, morate izdelati in uveljaviti pravilo za filtriranje na–Źel, ki omogo–Źa promet podatkov prek povezave. Pravilo **za filtriranje na–Źel** definira, kateri naslovi, protokoli in vrata lahko uporabljajo povezano povezavo.
3. **Definiranje vmesnika za pravila**
   Ko konfigurirate pravila paketov in vsa druga pravila, ki jih potrebujete, da omogo–Źite povezavo VPN, morate definirati vmesnik, za katerega jih boste uveljavili.
4. **Aktiviranje pravil paketov**
   Ko definirate vmesnik za pravila paketov, jih morate aktivirati, preden za┼ženete povezavo.
5. **Zagon povezave**
   To nalogo dokon–Źajte za zagon povezav, ki so inicializirane lokalno.

Konfiguriranje povezav VPN s pomo–Źjo –Źarovnika Nova povezava

–îarovnik Nova povezava omogo–Źa izdelavo navideznega zasebnega omre┼žja (VPN) med kakr┼ínokoli kombinacijo gostiteljev in prehodov. Na primer od gostitelja do gostitelja, od prehoda do gostitelja, od gostitelja do prehoda ali od prehoda do prehoda.

–îarovnik samodejno izdela vse konfiguracijske objekte, ki jih zahteva VPN za pravilno delovanje, kar vklju–Źuje tudi pravila paketov. Toda –Źe ┼želite v VPN dodati funkcijo, na primer bele┼ženje ali prevod omre┼žnega naslova za VPN (VPN NAT), boste najbr┼ž izbolj┼íali VPN s pomo–Źjo strani lastnosti ustrezne skupine dinami–Źnih klju–Źev ali povezave. V ta namen morate najprej zaustaviti povezavo, –Źe je le-ta aktivna. Nato z desno tipko mi┼íke kliknite skupino dinami–Źnih klju–Źev ali povezavo in izberite **Lastnosti**.

Preden za–Źnete, izpolnite svetovalca za na–Źrtovanje VPN. Svetovalec vam bo pomagal zbrati pomembne informacije, ki jih boste potrebovali za izdelavo VPN.

VPN izdelate s pomo–Źjo –Źarovnika za povezavo takole:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼žnik —>**Omre┼žje** —>**Na–Źela IP**.

2. Z desno tipko mi┼íke kliknite **Delo z navideznim zasebnim omre┼żjem** in izberite **Nova povezava**, da boste zagnali ─Źarovnika.
3. Izpolnite ─Źarovnika, da boste izdelali osnovno povezavo VPN. ─îe potrebujete pomo─Ź, kliknite **Pomo─Ź**.

Konfiguriranje na─Źel za za┼í─Źito VPN

Ko dolo─Žite, kako boste uporabljali VPN, morate definirati na─Źela za za┼í─Źito VPN. Posebej morate narediti naslednje:

- **Konfigurirati na─Źelo IKE (Internet Key Exchange)**
  Na─Źelo IKE definira, katero raven overjanja in za┼í─Žito ┼íifriranja bo uporabljal IKE med pogajanji prve faze. Prva faza IKE vzpostavi klju─Że za za┼í─Žito sporo─Žil, ki potujejo v nadaljnja pogajanja druge faze. Pri izdelavi ro─Źne povezave ni potrebno definirati na─Źela IKE. ─îe izdelate VPN s pomo─Žjo ─Źarovnika Nova povezava, lahko ─Źarovnik izdela na─Źelo IKE za vas.
- **Konfigurirati podatkovno na─Źelo**
  Podatkovno na─Źelo definira raven overjanja ali ┼íifriranja, ki ┼í─Žiti podatke na poti prek VPN. Komunicirajo─Ži sistemi se dogovorijo glede teh atributov med pogajanji druge faze protokola IKE (Internet Key Exchange). Pri izdelavi ro─Źne povezave ni potrebno definirati podatkovnega na─Źela. ─îe izdelate VPN s pomo─Žjo ─Źarovnika Nova povezava, lahko ─Źarovnik izdela podatkovno na─Źelo za vas.

Ko konfigurirate na─Źela za za┼í─Žito VPN, morate konfigurirati za┼í─Žitene povezave.

Konfiguriranje na─Źela IKE (Internet Key Exchange)

Na─Źelo IKE definira raven overjanja ali za┼í─Žito ┼íifriranja, ki jo uporablja IKE med prvo fazo pogajanj. Prva faza IKE vzpostavi klju─Że za za┼í─Žito sporo─Žil, ki potujejo v nadaljnja pogajanja druge faze. VPN overi pogajanja prve faze s pomo─Žjo podpisnega na─Žina RSA ali klju─Žev z vnaprej dolo─Ženo skupno rabo. ─îe nameravate overjati stre┼żnike klju─Žev z digitalnimi potrdili, jih morate najprej konfigurirati z Upravljalnikom digitalnih potrdil (mo┼żnost 5722-SS1 34). Na─Želo IKE dolo─Ža tudi, kateri oddaljeni stre┼żnik klju─Žev bo uporabljal to na─Źelo.

Naslednji koraki ka┼żejo, kako definirate na─Źelo IKE ali spremenite obstoje─Źega:

1. V Navigatorju iSeries(TM) raz┼íirite ikono va┼íega stre┼żnika **—> Omre┼żje—> Na─Źela IP—> Delo z navideznim zasebnim omre┼żjem—> Na─Źela za┼í─Žite IP**.
2. Za izdelavo novega na─Źela z desno tipko mi┼íke kliknite **Na─Źela Internet Key Exchange** in izberite **Novo na─Źelo Internet Key Exchange**. ─îe ┼żelite spremeniti obstoje─Że na─Źelo, kliknite v levem podoknu **Na─Źela Internet Key Exchange**, nato pa v desnem podoknu z desno tipko mi┼íke kliknite na─Źelo, ki ga ┼żelite spremeniti, in izberite **Lastnosti**.
3. Izpolnite vse strani lastnosti. ─îe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo─Ź**.
4. S klikom gumba **Potrdi** shranite spremembe.

Opomba: Priporo─Žamo, da vedno, ko uporabite klju─Ź z vnaprej dolo─Ženo souporabo za overjanje, uporabite pogajanje glavnega na─Žina. Ta nudi bolj za┼í─Žiteno izmenjavo. ─îe morate uporabiti klju─Że z vnaprej dolo─Ženo souporabo in pogajanje agresivnega na─Žina, uporabite zapletena gesla, ki jih je zelo te┼żko zlomiti v napadih, ki pregledujejo slovar. Priporo─Ženo je tudi, da redno spreminjate gesla. Za podrobnej┼íe informacije preberite zaslonsko pomo─Ź Navigatorja iSeries.

Konfiguriranje podatkovnega na─Źela

Podatkovno na─Źelo definira raven overjanja ali ┼íifriranja, ki ┼í─Žiti podatke na poti prek VPN. Komunicirajo─Ži sistemi dogovorijo te atribute med drugo fazo pogajanj protokola IKE (Internet Key Exchange).

Naslednji koraki ka┼żejo, kako definirate podatkovno na─Źelo ali spremenite obstoje─Źega:

1. V Navigatorju iSeries(TM) raz┼íirite ikono va┼íega stre┼żnika **—> Omre┼żje—> Na─Źela IP—> Delo z navideznim zasebnim omre┼żjem—> Na─Źela za┼í─Žite IP**.

2. Za izdelavo novega podatkovnega na─Źela z desno tipko mi┼íke kliknite **Podatkovna na─Źela** in izberite **Novo podatkovno na─Źelo**. ─Źe ┼żelite spremeniti obstoje─Će podatkovno na─Źelo, kliknite **Podatkovna na─Źela** (v levem podoknu), nato pa z desno tipko mi┼íke kliknite podatkovno na─Źelo, ki ga ┼żelite spremeniti (v desnem podoknu) in izberite **Lastnosti**.
3. Izpolnite vse strani lastnosti. ─Źe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo─Ź**.
4. S klikom gumba **Potrdi** shranite spremembe.

Konfiguriranje za┼í─Žitene povezave VPN

Ko konfigurirate na─Źela za┼í─Će za povezavo, morate konfigurirati za┼í─Žiteno povezavo. Za dinami─Źne povezave vklju─Źuje za┼í─Žiten povezovalni objekt skupino dinami─Źnih klju─Źev in povezavo prek dinami─Źnega klju─Ża.

Skupina dinami─Źnih klju─Źev definira splo┼íne zna─Žilnosti ene ali ve─Ć povezav VPN. Konfiguracija skupine dinami─Źnih klju─Źev omogo─Ża, da uporabite za vsako povezavo znotraj skupine ista na─Źela, toda razli─Źne podatkovne zaklju─Źne to─Żke. Skupina dinami─Źnih klju─Źev tudi omogo─Ża uspe┼íno pogajanje z oddaljenimi pobudniki, ─Će podatkovne zaklju─Źne to─Żke, ki jih predlaga oddaljeni sistem, niso vnaprej znane. To naredi s povezavo informacij na─Źel v skupini dinami─Źnih klju─Źev s pravili za filtriranje na─Źel s tipom dejanja IPSEC. ─Źe so dolo─Żene podatkovne zaklju─Źne to─Żke, ki jih ponudi oddaljeni pobudnik, znotraj obmo─Żja podanega pravila za filtriranje IPSEC, je za njih lahko uporabljeno na─Źelo, definirano v skupini dinami─Źnih klju─Źev.

Povezava prek dinami─Źnega klju─Ża definira zna─Žilnosti posameznih podatkovnih povezav med pari zaklju─Źnih to─Żk. Povezava prek dinami─Źnega klju─Ża obstaja znotraj skupine dinami─Źnih klju─Źev. Ko konfigurirate skupino dinami─Źnih klju─Źev, ki opisuje, katera na─Źela naj uporabijo povezave v skupini, morate izdelati posamezne povezave dinami─Źnega klju─Ża za povezave, ki jih boste inicializirali lokalno.

Za┼í─Žiten povezovalni objekt konfigurirate takole:

1. del: Konfiguracija skupine dinami─Źnih klju─Źev:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika **—> Omre┼żje—> Na─Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Žitene povezave**.
2. Z desno tipko mi┼íke kliknite **Po skupini** in izberite **Nova skupina dinami─Źnih klju─Źev**.
3. ─Źe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo─Ź**.
4. S klikom gumba **Potrdi** shranite spremembe.

2. del: Konfiguracija povezave dinami─Źnega klju─Ża

1. V Navigatorju iSeries raz┼íirite ikono stre┼żnika **—> Omre┼żje —> Na─Źela IP—> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Žitene povezave—> Po skupini**.
2. V levem podoknu Navigatorja iSeries z desno tipko mi┼íke kliknite skupino dinami─Źnih klju─Źev, ki ste jo izdelali v prvem delu, in izberite **Nova povezava dinami─Źnega klju─Ża**.
3. ─Źe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo─Ź**.
4. S klikom gumba **Potrdi** shranite spremembe.

Ko kon─Żate te korake, morate aktivirati pravila paketov, ki jih zahteva povezava za pravilno delovanje.

Opomba: Priporo─Żamo, da v ve─Źini primerov dopustite, da vmesnik VPN ustvari pravila paketov VPN samodejno; to naredite tako, da na strani **Skupina dinami─Źnega klju─Ża - Povezave** izberete mo┼żnost **Za to skupino ustvari naslednji filter na─Źel**. Toda ─Će izberete mo┼żnost **Pravilo za filtriranje na─Źel bo definirano v pravilih paketov**, morate konfigurirati pravila paketov VPN s pomo─Żjo urejevalnika pravil paketov in jih nato aktivirati.

Konfiguriranje ro–Źne povezave

Kot pove samo ime, je ro–Źna povezava tista, za katero morate konfigurirati vse lastnosti VPN ro–Źno. Poleg tega zahtevata oba konca povezave, da konfigurirate ve–Ź elementov, ki se morajo *natan–Źno* ujemati. Tako se morajo na primer vhodni klju–Źi ujemati z izhodnimi klju–Źi oddaljenega sistema, sicer povezava ne bo uspela.

Ro–Źne povezave uporabljajo stati–Źne klju–Že, ki se v –Źasu aktivnosti povezave ne osve┼żijo ali spremenijo. Ro–Źno povezavo morate zaustaviti, –Že ┼żelite spremeniti z njo povezan klju–Ź. –če menite, da to lahko povzro–Źi tveganje v za┼í–Źiti, in oba konca povezave podpirata protokol IKE (Internet Key Exchange), je morda bolje, da uporabite dinami–Źno povezavo.

Lastnosti ro–Źne povezave definirate takole:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika —**> Omre┼żje—> Na–Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í–Žitene povezave**.
2. Z desno tipko mi┼íke kliknite **Vse povezave** in izberite **Nova ro–Źna povezava**.
3. Izpolnite vse strani lastnosti. –če imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo–Ź**.
4. S klikom gumba **Potrdi** shranite spremembe.

Opomba: Priporo–Źamo, da v ve–Źini primerov dopustite, da vmesnik VPN samodejno izdela pravila paketov VPN; to naredite tako, da na strani **Ro–Źna povezava - Povezava** izberete mo┼żnost **Ustvari filter na–Źel, ki se ujema s podatkovnimi zaklju–Źnimi to–Źkami**. Toda –Že izberete mo┼żnost **Pravilo za filtriranje na–Źel bo definirano v pravilih paketov**, morate ro–Źno konfigurirati pravila za filtriranje na–Źel in jih nato aktivirati.

Konfiguriranje pravil paketov VPN

–če povezavo izdelujete prvi–Ź, pustite, da VPN samodejno ustvari pravila paketov VPN. To lahko naredite s pomo–Žjo –Źarovnika Nova povezava ali na straneh lastnosti VPN, kjer konfigurirate povezavo.

–če ste se odlo–Žili, da boste izdelali pravila paketov VPN s pomo–Žjo urejevalnika pravil paketov v Navigatorju iSeries(TM), izdelajte na ta na–Žin tudi vsa dodatna pravila. –če pa ste pustili, da je pravila za filtriranje na–Źel izdelal VPN, izdelajte na ta na–Žin tudi dodatna pravila za filtriranje na–Źel.

Na splo┼íno zahteva VPN dve vrsti pravil za filtriranje: pravila za filtriranje pred IPSec in pravila za filtriranje na–Źel. Preberite spodnje teme in se nau–Žite, kako konfigurirati ta pravila s pomo–Žjo urejevalnika pravil paketov v Navigatorju iSeries. –če ┼żelite informacije o drugih mo┼żnosti filtriranja in VPN, preberite razdelek teme Koncepti VPN z naslovom *VPN in filtriranje IP*.

- **Pravila pred IPSec**
  Pravila pred IPSec so vsa pravila v sistemu, ki so pred pravili s tipom dejanja IPSEC. V tej temi bomo razlo┼żili samo pravila pred IPSec, ki jih zahteva VPN za pravilno delovanje. V tem primeru so pravila pred IPSec par pravil, ki omogo–Źajo povezavo IKE prek povezave. IKE omogo–Źa dinami–Źno tvorbo klju–Źev in pogajanja za povezavo. Druga pravila pred IPSec dodajte glede na dolo–Źeno omre┼żno okolje in na–Želo za┼í–Žite.

  Opomba: To vrsto pravila pred IPSec morate konfigurirati samo, –Že ┼że imate druga pravila, ki dovoljujejo IKE za dolo–Žene sisteme. –če v sistemu ne obstajajo nobena pravila za filtriranje, ki bi izrecno dovoljevala promet IKE, je le-ta implicitno dovoljen.
- **Pravilo za filtriranje na–Źel**
  Pravilo za filtriranje na–Źel definira promet, ki lahko uporablja VPN, in na–Želo za za┼í–Žito podatkov, ki bo uveljavljeno za ta promet.

Preden za–Źnete

–če vmesniku dodate pravila za filtriranje, sistem za ta vmesnik samodejno doda privzeto pravilo ZAVRNI. To pomeni, da je zavrnjen ves promet, ki ni izrecno dovoljen. Tega pravila ne morete prikazati ali spremeniti. Posledi–Źno boste lahko ugotovili, da promet, ki se je predhodno –Źudno vedel, po aktiviranju pravil za filtriranje VPN ne bo ve–Ź deloval. –če ┼żelite za vmesnik poleg VPN omogo–Žiti tudi drug promet, morate dodati izrecna pravila DOVOLI.

Ko konfigurirate ustrezna pravila za filtriranje, morate definirati vmesnik, za katerega jih boste uveljavili, nato pa jih aktivirati.

Bistvenega pomena, da pravila za filtriranje pravilno konfigurirate. V nasprotnem primeru lahko namre─Ź zablokirajo ves vhodni in izhodni promet IP na iSeries. To vklju─Źuje povezave z Navigatorjem iSeries, ki jih uporabljate za konfiguriranje pravil za filtriranje.

─ie pravila za filtriranje ne dovoljujejo prometa Navigatorja iSeries, Navigator iSeries ne more komunicirati z iSeries. ─ie se znajdete v tak┼íni situaciji, se morate prijaviti v iSeries s pomo─Źjo vmesnika, ki ima ┼íe vedno vzpostavljeno povezljivost, kot je na primer operacijska ukazna miza. Za odstranitev vseh filtrov v tem sistemu uporabite ukaz RMVTCPTBL. Ta ukaz tudi zaustavi stre┼żnike *VPN in jih znova za┼żene. Nato konfigurirajte filtre in jih znova aktivirajte.

Konfiguriranje pravil za filtriranje pred IPSec

Opozorilo: To nalogo opravite samo, ─Če ste podali, naj VNP ne ustvari pravil za filtriranje na─Źel samodejno.

Par stre┼żnikov IKE (Internet Key Exchange) dinami─Źno dogovori in osve┼żi klju─Że. IKE uporablja znana vrata 500. ─ie ┼żelite, da bo IKE pravilno deloval, morate za ta promet IP dovoliti datagrame UDP prek vrat 500. V ta namen morate izdelati par pravil za filtriranje: enega za vhodni, drugega pa za izhodni promet, da lahko va┼ía povezava dinami─Źno dogovori klju─Że za za┼í─Žito povezave:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik **—>Omre┼żje —>Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Urejevalnik pravil**. S tem boste odprli urejevalnik pravil paketov, v katerem lahko izdelate ali urejate pravila filtriranja in NAT za iSeries.
3. V uvodnem oknu izberite **Izdelaj novo datoteko pravil paketov** in kliknite **Potrdi**.
4. V urejevalniku pravil paketov izberite **Vstavi —>Filter**.
5. Na strani **Splo┼íno** podajte ime niza za pravila filtriranja VPN. Priporo─Źamo, da izdelate vsaj tri razli─Źne nize: enega za pravila filtriranja pred IPSec, drugega za pravila za filtriranje na─Źel in tretjega za me┼íana pravila filtriranja DOVOLI in ZAVRNI. Poimenujte niz, ki vsebuje pravila za filtriranje pred IPSec in mu dodajte predpono *preipsec*. Na primer preipsecfilters.
6. V polju **Dejanje** izberite s spustnega seznama **DOVOLI**.
7. V polju **Smer** izberite s spustnega seznama **IZHOD**.
8. V polju **Izvorni naslov** izberite s spustnega seznama **=** in v drugo polje vnesite naslov IP lokalnega stre┼żnika klju─Źev. Podali ste naslov IP lokalnega stre┼żnika klju─Źev v na─Źelu IKE.
9. V polju **Ciljni naslov** izberite s spustnega seznama **=** in v drugo polje vnesite naslov IP oddaljenega stre┼żnika klju─Źev. Podali ste tudi naslov IP oddaljenega stre┼żnika klju─Źev v na─Źelu IKE.
10. Na strani **Storitve** izberite **Storitev**. S tem omogo─Źite polja **Protokol**, **Izvorna vrata** in **Ciljna vrata**.
11. V polju **Protokol** izberite s spustnega seznama **UDP**.
12. Za **Izvorna vrata** izberite v prvem polju **=**, nato pa v drugo polje vnesite 500.
13. Ponovite prej┼ínji korak ┼íe za **Ciljna vrata**.
14. Kliknite **Potrdi**.
15. Te korake ponovite ┼íe za vhodni filter. Uporabite isto ime niza in po potrebi zamenjajte naslove.

Opomba: Manj varna, toda preprostej┼ía mo┼żnost za dovolitev prometa IKE prek povezave je, da konfigurirate samo filter pred IPSec, in v poljih **Smer**, **Izvorni naslov** in **Ciljni naslov** uporabite univerzalni znak (*).

Naslednji korak je konfiguracija pravila za filtriranje na─Źel, ki definira, kateri promet IP ┼í─Žiti povezava IPN.

Konfiguriranje pravil za filtriranje na─Źel

Opozorilo: To nalogo opravite samo, ─Če ste podali, naj VNP ne ustvari pravila za filtriranje na─Źel samodejno.

Pravilo za filtriranje na–Źel (pravilo, kjer je dejanje=IPSEC) definira, kateri naslovi, protokoli in vrata lahko uporabljajo VPN. Dolo–Źa tudi na–Żelo, ki bo uporabljeno za promet povezave VPN. Takole konfigurirate pravila za filtriranje na–Źel:

Opomba: –îe ste pravkar konfigurirali pravilo pred IPSec (samo za dinami–Źne povezave), bo urejevalnik pravil paketov ┼íe vedno odprt; pojdite na –Źetrti korak.

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik —>**Omre┼żje** —>**Na–Żela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Urejevalnik pravil**. S tem boste odprli urejevalnik pravil paketov, v katerem lahko izdelate ali urejate pravila filtriranja in NAT za iSeries.
3. V uvodnem oknu izberite **Izdelaj novo datoteko pravil paketov** in kliknite **Potrdi**.
4. V urejevalniku pravil paketov izberite **Vstavi** —>**Filter**.
5. Na strani **Splo┼íno** podajte ime niza za pravila filtriranja VPN. Priporo–Źamo, da izdelate vsaj tri razli–Źne nize: enega za pravila filtriranja pred IPSec, drugega za pravila za filtriranje na–Źel in tretjega za me┼íana pravila filtriranja DOVOLI in ZAVRNI. Na primer filtrina–Źel
6. V polju **Dejanje** izberite s spustnega seznama **IPSEC**. Polje **Smer** je po privzetku nastavljeno na IZHOD in ga ne morete spremeniti. –îeprav je privzeta vrednost tega polja nastavljena na IZHOD, je v resnici dvosmerno. Mo┼żnost IZHOD je prikazana, da se razjasni semantika vhodnih vrednosti. Izvorne vrednosti so na primer lokalne vrednosti, ciljne vrednosti pa oddaljene vrednosti.
7. Za **Izvorni naslov** izberite v prvem polju **=**, nato pa v drugo polje vnesite naslov IP lokalne podatkovne zaklju–Źne to–Źke. Podate lahko tudi obmo–Źje naslovov IP ali naslov IP in masko podmre┼że, ko jih definirate s pomo–Źjo funkcije **Definiraj naslove**.
8. Za **Ciljni naslov** izberite v prvem polju **=**, nato pa v drugo polje vnesite naslov IP oddaljene zaklju–Źne podatkovne to–Źke. Podate lahko tudi obmo–Źje naslovov IP ali naslov IP in masko podmre┼że, ko jih definirate s pomo–Źjo funkcije **Definiraj naslove**.
9. V polju **Bele┼żenje** podajte zahtevano raven bele┼żenja.
10. V polju **Ime povezave** izberite definicijo povezave, za katero bodo uveljavljena ta pravila za filtriranje.
11. (izbirno) Vnesite opis.
12. Na strani **Storitve** izberite **Storitev**. S tem omogo–Źite polja **Protokol**, **Izvorna vrata** in **Ciljna vrata**.
13. V poljih **Protokol**, **Izvorna vrata** in **Ciljna vrata** izberite ustrezno vrednost za promet. Namesto tega lahko s spustnega seznama izberete tudi zvezdico (*). S tem omogo–Źite, da uporabi VPN katerokoli protokol, ki uporabi katerakoli vrata.
14. Kliknite **Potrdi**.

Naslednji korak je definiranje vmesnika, za katerega boste uveljavili ta pravila za filtriranje.

Opomba: Ko dodate pravila filtriranja za vmesnik, sistem za vmesnik samodejno doda privzeto pravilo ZAVRNI. To pomeni, da je zavrnjen ves promet, ki ni izrecno dovoljen. Tega pravila ne morete prikazati ali spremeniti. Posledi–Źno boste lahko ugotovili, da povezave, ki so se prej –Źudno vedle, po aktiviranju pravil paketov VPN ne bodo ve–Ź delovale. –îe ┼żelite za vmesnik poleg VPN omogo–Źiti tudi drug promet, morate dodati izrecna pravila DOVOLI.

Definiranje vmesnika za pravila filtriranja VPN

Ko konfigurirate pravila paketov VPN in vsa druga pravila, ki so potrebna, da omogo–Źite povezavo VPN, morate definirati vmesnik, za katerega jih boste uveljavili.

Vmesnik, za katerega boste uveljavili pravila za filtriranje VPN, definirate takole:

Opomba: –îe ste pravkar konfigurirali pravila paketov VPN, bo vmesnik pravil paketov ┼íe vedno odprt; pojdite na –Źetrti korak.

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik —>**Omre┼żje** —>**Na–Żela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Urejevalnik pravil**. S tem boste odprli urejevalnik pravil paketov, v katerem lahko izdelate ali urejate pravila filtriranja in NAT za iSeries.
3. V uvodnem oknu izberite **Izdelaj novo datoteko pravil paketov** in kliknite **Potrdi**.

4. V urejevalniku pravil paketov izberite **Vstavi —> Vmesnik filtrov**.
5. Na strani **Splo┼íno** izberite **Ime linije**, nato pa s spustnega seznama izberite opis linije, na katerega se nana┼íajo pravila paketov VPN.
6. (izbirno) Vnesite opis.
7. Na strani **Nizi filtrov** kliknite **Dodaj**, da boste dodali vse nize imen za pravkar konfigurirane filtre.
8. Kliknite **Potrdi**.
9. Shranite datoteko pravil. Datoteka je shranjena v integrirani datote─Źni sistem v iSeries s pripono .i3p.
   Opomba: Datoteke ne shranite v naslednji imenik:

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

   Ta imenik je namenjen samo za sistemsko uporabo. ─îe morate kdaj s pomo─Źjo ukaza RMVTCPTBL *ALL deaktivirati pravila paketov, bo ukaz zbrisal vse datoteke znotraj tega imenika.

Ko definirate vmesnik za pravila filtriranja, jih morate aktivirati, preden lahko za┼żenete VPN.

Aktiviranje pravil paketov VPN

Preden lahko za┼żenete povezave VPN, morate aktivirati pravila paketov VPN. Pravil paketov ne morete aktivirati (deaktivirati), ─Źe se povezave VPN izvajajo v sistemu. Zato pred aktiviranjem pravil za filtriranje VPN zagotovite, da niso z njimi povezane nobene aktivne povezave.

─îe ste izdelali povezave VPN s ─Źarovnikom Nova povezava, lahko izberete samodejno aktiviranje pravil. V primeru, da so v kateremkoli podanem vmesniku aktivna druga pravila paketov, ne pozabite, da jih bodo pravila za filtriranje paketov VPN nadomestila.

─îe izberete aktiviranje pravil, ustvarjenih z VPN, s pomo─Źjo urejevalnika pravil paketov, naredite naslednje korake:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik **—>Omre┼żje —>Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Aktiviraj**. Odpre se pogovorno okno **Aktiviranje pravil paketov**.
3. Izberite, ali ┼żelite aktivirati samo pravila, ustvarjena z VPN, samo izbrano datoteko ali pravila, ustvarjena z VPN in izbrano datoteko. Zadnje lahko na primer izberete, ─Źe imate me┼íana pravila DOVOLI in ZAVRNI, ki jih ┼żelite uveljaviti za vmesnik poleg pravil, ustvarjenih z VPN.
4. Izberite vmesnik, za katerega ┼żelite aktivirati pravila. Izberete lahko aktiviranje v dolo─Źenem vmesniku, v identifikatorju od to─Źke do to─Źke ali v vseh vmesnikih in identifikatorjih od to─Źke do to─Źke.
5. V pogovornem oknu kliknite **Potrdi** in potrdite, da ┼żelite preveriti in aktivirati pravila v podanem vmesniku ali vmesnikih. Ko kliknete Potrdi, sistem preveri skladnjo in semanti─Źne napake v pravilih in sporo─Źi rezultate v sporo─Źilnem oknu na dnu urejevalnika. Za sporo─Źila o napakah, ki so povezana z dolo─Źeno datoteko ali ┼ítevilko vrstice, lahko z desno tipko mi┼íke kliknete napako in izberete **Pojdi na vrstico**, da boste ozna─Źili napako v datoteki.

Ko aktivirate pravila za filtriranje, lahko za┼żenete povezavo VPN.

Zagon povezave VPN

Navodila so napisana na domnevi, da ste pravilno konfigurirali povezavo VPN. Naslednji koraki ka┼żejo, kako za┼żenete povezavo VPN:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik **—>Omre┼żje —>Na─Źela IP**.
2. ─îe stre┼żnik VPN ni zagnan, z desno tipko mi┼íke kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Za┼żeni**. S tem za┼żenete stre┼żnik VPN.
3. Preverite, ali so pravila paketov aktivirana.
4. Raz┼íirite **Delo z navideznim zasebnim omre┼żjem—> Za┼í─Žitene povezave**.
5. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
6. Z desno tipko mi┼íke kliknite povezavo, ki jo ┼żelite zagnati in izberite **Za┼żeni**. ─îe ┼żelite zagnati ve─Ź povezav, jih izberite, kliknite z desno tipko mi┼íke in izberite **Za┼żeni**.

Upravljanje VPN

S pomo─Źjo vmesnika VPN Navigatorja iSeries(TM) lahko vodite vse naloge upravljanja, ki vklju─Źujejo naslednje:

- **Zagon povezave VPN**
  To nalogo izpolnite za zagon povezav, ki jih boste inicializirali lokalno.
- **Nastavitev privzetih atributov povezav**
  Privzete vrednosti izpolnijo okna, ki jih uporabite za izdelavo novih na─Źel in povezav. Privzete vrednosti lahko nastavite za ravni za┼í─Źite, upravljanje sej klju─Źev, trajanje klju─Źev in trajanje povezav.
- **Vnovi─Źna nastavitev povezav v stanju napake**
  Vnovi─Źna nastavitev povezav v stanju napake povzro─Źi njihovo vrnitev v stanje mirovanja.
- **Prikaz informacij o napaki**
  To nalogo izpolnite, da vam bo pomagala dolo─Źiti, zakaj je v povezavi napaka.
- **Prikaz atributov aktivnih povezav**
  To nalogo izpolnite, da boste preverili status in druge atribute aktivnih povezav.
- **Uporaba sledenja stre┼żnika VPN**
  Sledenje stre┼żnika VPN omogo─Ża, da konfigurirate, za┼żenete, zaustavite in prika┼żete sledenja Upravljalnika povezav VPN in stre┼żnika Upravljalnika klju─Źev VPN. To je podobno uporabi ukaza TRCTCPAPP *VPN na znakovno osnovanem vmesniku z razliko, da si lahko ogledate sledenje, ko je povezava aktivna.
- **Prikaz dnevnikov opravil stre┼żnika VPN**
  Tem navodilom sledite za prikaz dnevnikov opravil za Upravljalnik klju─Źev VPN in Upravljalnik povezav VPN.
- **Zaustavitev povezav**
  To nalogo izpolnite za zaustavitev aktivnih povezav.
- **Prikaz atributov dogovorov za za┼í─Źito (SA)**
  To nalogo izpolnite, da boste prikazali atribute dogovorov za za┼í─Źito (SA-jev), ki so povezani z omogo─Ćeno povezavo.
- **Brisanje konfiguracijskih objektov VPN**
  Preden zbri┼íete konfiguracijski objekt VPN iz baze podatkov na─Źel VPN, morate razumeti, kako to vpliva na druge povezave in skupine povezav VPN.

Nastavitev privzetih atributov za povezave

Pri za─Źetni izdelavi novih objektov VPN izpolnijo privzete vrednosti za┼í─Źite razli─Źna polja.

Privzete vrednosti za┼í─Źite za povezave VPN nastavite takole:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik **—>Omre┼żje —>Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Delo z zasebnim navideznim omre┼żjem** in izberite **Privzetki**.
3. ─Źe imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo─Ź**.
4. Ko izpolnite vse strani lastnosti, kliknite **Potrdi** .

Vnovi─Źna nastavitev povezav v stanju napake

Naslednji koraki ka┼żejo, kako osve┼żite povezavo, ki je v stanju napake:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika **—> Omre┼żje—> Na─Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite povezavo, ki jo ┼żelite nastaviti na novo, in kliknite **Nastavi na novo**. S tem nastavite povezavo v stanje mirovanja. ─Źe ┼żelite na novo nastaviti ve─Ź povezav v stanju napake, jih izberite, kliknite z desno tipko mi┼íke in izberite **Nastavi na novo**.

Prikaz informacij o napaki

─Źe si ┼żelite ogledati informacije o povezavah, v katerih je pri┼ílo do napake, opravite naslednje korake:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika —> **Omre┼żje—> Na–Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í–Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite ┼żeleno povezavo, v kateri je pri┼ílo do napake, in izberite **Informacije o napaki**.

Prikaz atributov aktivne povezave

Naslednji koraki ka┼żejo, kako prika┼żete trenutne atribute aktivne povezave ali povezave na zahtevo:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika —> **Omre┼żje—> Na–Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í–Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite aktivno povezavo ali povezavo na zahtevo, ki si jo ┼żelite ogledati, in izberite **Lastnosti.**
4. Odprite stran **Trenutni atributi** in si oglejte atribute povezave.

Atribute vseh povezav si lahko ogledate tudi v oknu Navigatorja iSeries. Po privzetku so prikazani samo atributi statusa, opisa in vrste povezave. Naslednji koraki ka┼żejo, kako spremenite podatke, ki so prikazani:

1. V Navigatorju iSeries raz┼íirite ikono va┼íega stre┼żnika —> **Omre┼żje—> Na–Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í–Źitene povezave**.
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z menija **Objekti** izberite **Stolpci**. Odpre se pogovorno okno, v katerem lahko izberete, katere atribute ┼żelite prikazati v oknu Navigatorja iSeries.

–ie spremenite stolpce za prikaz, ne pozabite, da te spremembe niso specifi–Źne za dolo–Źenega uporabnika ali PC, pa–Ź pa za celoten sistem.

Uporaba sledenja stre┼żnika VPN

Naslednji koraki ka┼żejo, kako prika┼żete sledenje stre┼żnika VPN:

1. V Navigatorju iSeries(TM) raz┼íirite stre┼żnik —>**Omre┼żje** —>**Na–Źela IP**.
2. Z desno tipko mi┼íke kliknite **Delo z navideznim zasebnim omre┼żjem**,izberite **Diagnosti–Źna oro┼żja**, nato pa **Sledenje stre┼żnika**.

Naslednji koraki ka┼żejo, kako podate, kak┼íno vrsto sledenja naj izdelata Upravljalnik klju–Źev VPN in Upravljalnik povezav VPN:

1. V oknu **Delo z navideznim zasebnim omre┼żjem** kliknite

   (Mo┼żnosti).
2. Na strani **Upravljalnik povezav** podajte, kak┼íno vrsto sledenja naj izvaja stre┼żnik Upravljalnika povezav.
3. Na strani **Upravljalnik klju–Źev** podajte, kak┼íno vrsto sledenja naj izvaja stre┼żnik Upravljalnika klju–Źev.
4. –ie imate vpra┼íanja o tem, kako izpolniti stran ali njena polja, kliknite **Pomo–Ź**.
5. S klikom gumba **Potrdi** shranite spremembe.
6. Sledenje za┼żenite s klikom na

   (Za┼żeni). –ie si ┼żelite ogledati najnovej┼íe informacije sledenja, ob–Źasno kliknite

   (Osve┼żi).

Prikaz dnevnikov opravil stre┼żnika VPN

Naslednji koraki ka┼żejo, kako prika┼żete trenutne dnevnike opravil Upravljalnika klju─Źev VPN ali Upravljalnika povezav VPN:

1. V Navigatorju iSeries(TM) raz┼íirite ikono va┼íega stre┼żnika **—> Omre┼żje—> Na─Źela IP**
2. Z desno tipko mi┼íke kliknite **Delo z navideznim zasebnim omre┼żjem** in izberite **Diagnosti─Źna orodja**, nato pa izberite dnevnik opravil stre┼żnika, ki si ga ┼żelite ogledati.

Prikaz atributov dogovorov za za┼í─Źito (SA)

Naslednji koraki ka┼żejo, kako prika┼żete atribute dogovorov za za┼í─Źito (SA-jev), ki so povezani z omogo─Ćeno povezavo:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika **—> Omre┼żje—> Na─Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite ustrezno aktivno povezavo in izberite **Dogovori za za┼í─Źito.**V nastalem oknu si lahko ogledate lastnosti vseh dogovorov za za┼í─Źito, povezanih z dolo─Ćeno povezavo.

Zaustavitev povezave VPN

Naslednji koraki ka┼żejo, kako zaustavite aktivno povezavo ali povezavo s stanjem v ─Źakanju:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika **—> Omre┼żje—> Na─Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite povezavo, ki jo ┼żelite zaustaviti, in izberite **Zaustavi**. ─Źe ┼żelite zaustaviti ve─Ź povezav, jih izberite, kliknite z desno tipko mi┼íke in izberite **Zaustavi**.

Brisanje konfiguracijskih objektov VPN

─Źe ste prepri─Źani, da morate zbrisati povezavo VPN iz baze podatkov na─Źel VPN, opravite naslednje korake:

1. V Navigatorju iSeries(TM) raz┼íirite ikono stre┼żnika **—> Omre┼żje—> Na─Źela IP> Delo z navideznim zasebnim omre┼żjem—> Za┼í─Źitene povezave**
2. Kliknite **Vse povezave**, da boste v desnem podoknu prikazali seznam povezav.
3. Z desno tipko mi┼íke kliknite povezavo, ki jo ┼żelite zbrisati, in izberite **Zbri┼íi**.

Odpravljanje te┼żav v VPN

VPN je zapletena in hitro spreminjajo─Ća se tehnologija, ki zahteva vsaj osnovno poznavanje standardnih tehnologij IPSec. Poznati morate tudi pravila za filtriranje IP, saj VPN zahteva za pravilno delovanje ve─Ć pravil za filtriranje. Zaradi te zapletenosti boste v povezavah VPN ob─Źasno naleteli na te┼żave. Odpravljanje te┼żav v VPN ni vedno preprosto. Razumeti morate sistem in omre┼żna okolja, kot tudi komponente, s pomo─Źjo katerih jih upravljate. V naslednjih temah boste na┼íli nasvete o odpravljanju razli─Źnih te┼żav, na katere lahko naletite pri uporabi VPN:

- **Za─Źetek odpravljanja te┼żav v VPN**
  Sem pojdite, da boste na┼íli te┼żavo v povezavah VPN in jo odpravili.
- **Splo┼íne konfiguracijske napake VPN in kako jih odpraviti**
  Tema vsebuje najpogostej┼íe uporabni┼íke napake in nudi mo┼żne re┼íitve.
- **Odpravljanje te┼żav v VPN z dnevnikom QIPFILTER**
  Tema vsebuje informacije o pravilih za filtriranje VPN.
- **Odpravljanje te┼żav v VPN z dnevnikom QVPN**
  Tema vsebuje informacije o prometu in povezavah IP.
- **Odpravljanje te┼żav v VPN z dnevniki opravil VPN**
  Tema opisuje razli─Źne dnevnike opravil, ki jih uporablja VPN.
- **Odpravljanje te┼żav v VPN s komunikacijskim sledenjem OS/400(R)**
  Tema opisuje, kako slediti podatkom v komunikacijski liniji.

Za–Źetek odpravljanja te┼žav v VPN

Te┼žave v VPN lahko za–Źnete analizirati na ve–Ź na–Źinov:

1. Vedno preverite, ali ste uveljavili najnovej┼íe za–Źasne popravke programa (PTF-je).
2. Preverite, ali va┼í sistem zadovoljuje minimalne zahteve za nastavitev VPN.
3. Preglejte vsa sporo–Źila o napakah, ki jih najdete v oknu Informacije o napaki ali v dnevnikih opravil stre┼żnika VPN za lokalne in oddaljene sisteme. Pravzaprav je pri odpravljanju te┼žav v povezavah VPN pogosto potrebno preveriti oba konca povezave. Poleg tega morate preveriti ┼ítiri naslove: lokalno in oddaljeno zaklju–Źno to–Źko povezave - naslova, kjer je IPSec uveljavljen za pakete IP, in lokalno in oddaljeno podatkovno zaklju–Źno to–Źko - izvorni in ciljni naslov paketov IP.
4. –îe sporo–Źila o napakah ne nudijo dovolj informacij za re┼íitev te┼žave, preglejte ┼íe dnevnik filtriranja IP.
5. Tudi v komunikacijskem sledenju iSeries(TM) lahko najdete splo┼íne informacije o tem, ali lokalni sistem sprejme ali po┼ílje povezovalne zahteve.
6. Drug na–Źin za osamitev te┼žav nudi tudi ukaz TRCTCPAPP (Sledenje aplikaciji TCP). IBM(R)-ova servisna slu┼žba obi–Źajno uporablja TRCTCPAPP za pridobitev izhodnih podatkov sledenja, da lahko analizira te┼žave v povezavi.

Druge stvari, ki jih je potrebno preveriti

–îe pride po nastavitvi povezave do napake in niste prepri–Źani, kje v omre┼żju je te┼žava, poskusite poenostaviti svoje okolje. Namesto da na primer naenkrat pregledate vse dele povezave VPN, za–Źnite s samo povezavo IP. Naslednji seznam nudi nekaj osnovnih smernic, ki ka┼żejo, kako za–Źeti analizo te┼žave VPN od najpreprostej┼íe povezave IP do najzapletenej┼íih povezav VPN:

1. Za–Źnite s konfiguriranjem IP med lokalnim in oddaljenim gostiteljem. Odstranite vse filtre IP vmesnika, s pomo–Źjo katerih komunicirata lokalni in oddaljeni sistem. Ali lahko v lokalnem gostitelju izvedete ukaz PING za oddaljenega gostitelja?

   Opomba: Ne pozabite na poziv za ukaz PING; vnesite naslov oddaljenega sistema, s pomo–Źjo PF10 vnesite dodatne parametre, nato pa vnesite ┼íe lokalni naslov IP. To je ┼íe posebej pomembno, –Źe imate ve–Ź fizi–Źnih ali logi–Źnih vmesnikov. S tem zagotovite, da so v pakete PING postavljeni pravilni naslovi.

   –îe odgovorite z **da**, nadaljujte z drugim korakom. –îe odgovorite z **ne**, preverite konfiguracijo IP, status vmesnika in postavke usmerjanja. –îe je konfiguracija pravilna, s pomo–Źjo komunikacijskega sledenja na primer preverite, ali zahteva PING zapusti sistem. –îe po┼íljete zahtevo PING, vendar ne prejmete odgovora, je te┼žava najbr┼ż v omre┼żju ali v oddaljenem sistemu.

   Opomba: Morda obstajajo vmesni usmerjevalniki ali po┼żarni zid, ki izvajajo filtriranje paketov IP in tudi paketov PING. PING zna–Źilno temelji na protokolu ICMP. –îe ukaz PING uspe, veste, da ste vzpostavili povezljivost. –îe PING ne uspe, veste samo, da PING ni uspel. Za preverjanje povezljivosti je najbolje, da med dvema sistemoma preizkusite ┼íe druge protokole IP kot sta Telnet ali FTP.
2. Preverite pravila filtriranja za VPN in zagotovite, da so aktivirana. Ali se filtriranje uspe┼íno za┼żene? –îe odgovorite z **da**, nadaljujte s tretjim korakom. –îe odgovorite z **ne**, preverite sporo–Źila o napakah v oknu Pravila paketov Navigatorja iSeries. Zagotovite, da pravila filtriranja ne podajajo prevoda omre┼żnega naslova (NAT) za noben promet VPN.
3. Za┼żenite povezavo VPN. Ali se povezava uspe┼íno za┼żene? –îe odgovorite z **da**, nadaljujte s –Źetrtim korakom. –îe odgovorite z **ne**, preglejte, ali je v dnevniku opravil QTOVMAN in dnevnikih opravil QTOKVPNIKE zabele┼żena kak┼ína napaka.
   –îe uporabljate VPN, morajo ponudnik internetnih storitev (ISP) in vsi za┼í–Źitni prehodi v omre┼żji podpirati protokola AH (Authentication Header) in ESP (Encapsulated Security Payload). Ali boste izbrali AH ali ESP je odvisno od predlogov, ki jih definirate za povezavo VPN.
4. Ali lahko prek povezave VPN aktivirate uporabni┼íko sejo? –îe odgovorite z **da**, povezava VPN deluje kot je potrebno. –îe odgovorite z **ne**, preverite, ali v pravilih paketov, v skupini dinami–Źnih klju–Źev VPN ter v povezavah obstajajo definicije filtrov, ki ne dopu┼í–Źajo ┼żelenega uporabni┼íkega prometa.

Splo┼íne konfiguracijske napake VPN in kako jih odpraviti

Razdelek opisuje nekaj splo┼ínih te┼żav, ki se pojavljajo v VPN, in povezave z nasveti za njihovo re┼íitev.

Opomba: Ko konfigurirate VPN, dejansko izdelate ve─Ź razli─Źnih konfiguracijskih objektov, ki jih VPN zahteva, da omogo─Či povezavo. V dolo─Źbah GUI VPN so ti objekti na─Źela za┼í─Źite IP in varne povezave. ─Źe v teh informacijah omenimo objekt, pomeni, da gre za enega ali ve─Ź teh delov VPN.

Splo┼ína sporo─Źila o napakah, na katere lahko naletite

Sporo─Źilo	Simptom
TCP5B28	─Źe poskusite aktivirati pravila za filtriranje za vmesnik, ─Źe prika┼że naslednje sporo─Źilo: kr┼íitev vrstnega reda TCP5B28 CONNECTION_DEFINITION
Postavka ni bila najdena	─Źe z desno tipko mi┼íke kliknete objekt VPN in izberete **Lastnosti** ali **Zbri┼íi**, se prika┼że sporo─Źilo, ki pravi, da **postavka ni bila najdena**.
PARAMETER PINBUF NI VELJAVEN	Ko poskusite zagnati povezavo, se prika┼że sporo─Źilo, ki pravi, da **PARAMETER PINBUF NI VELJAVEN...**
Postavka ni bila najdena, oddaljen stre┼żnik klju─Źev...	─Źe izberete **Lastnosti** za povezavo z dinami─Źnim klju─Źem, se prika┼że sporo─Źilo o napaki, ki pravi, da stre┼żnik ne more najti podanega oddaljenega stre┼żnika klju─Źev.
Objekta ni mogo─Će a┼żurirati	─Źe izberete na strani lastnosti za skupino z dinami─Źnim klju─Źem ali ro─Źno povezavo **Potrdi**, se prika┼że sporo─Źilo, ki pravi, da sistem ne more a┼żurirati objekta.
Klju─Źa ni mogo─Će ┼íifrirati...	Prika┼że se sporo─Źilo, ki pravi, da sistem ne more ┼íifrirati klju─Źev, ker mora biti vrednost QRETSVRSEC nastavljena na 1.
CPF9821	Ko poskusite raz┼íiriti ali odpreti vsebnik na─Źel IP v Navigatorju iSeries(TM), se prika┼że sporo─Źilo CPF9821- Nimate pooblastila za program QTFRPRS v knji┼żnici QSYS.

Druge te┼żave, na katere lahko naletite

Napaka	Simptom
Vsi klju─Źi so prazni	Ko prika┼żete lastnosti za ro─Źno povezavo, so vsi klju─Źi z vnaprej dolo─Ženo skupno rabo in klju─Źi algoritmov za povezavo prazni.
Prika┼że se prijava za drug sistem	Pri prvi uporabi vmesnika pravil paketov v Navigatorju iSeries se prika┼że prijavni zaslon za sistem, ki ni trenutni.
Ni statusa povezave	Povezava nima v stolpcu **Status** okna Navigatorja iSeries nobene vrednosti.
Zaustavljene povezave so ┼íe vedno omogo─Žene	Ko zaustavite povezave, ka┼że okno Navigatorja iSeries da je povezava ┼íe vedno omogo─Žena.
3DES ni na voljo za ┼íifriranje	─Źe delate s pretvorbo na─Źel IKE, s pretvorbo podatkovnih na─Źel ali z ro─Źno povezavo, ni na voljo algoritem ┼íifriranja 3DES.
Prika┼żejo se nepri─Źakovani stolpci	Nastavili ste stolpce, ki jih ┼żelite prikazati v oknu Navigatorja iSeries za povezave VPN, toda ko si okno ogledate kasneje, so prikazani drugi stolpci.

Aktivnih pravil za filtriranje ni mogo–Źe deaktivirati	Ko poskusite deaktivirati trenutni niz pravil za filtriranje, se v oknu rezultatov prika┼že sporo–Žilo Aktivnih pravil ni mogo–Źe deaktivirati.
Skupina dinami–Źnih klju–Źev za povezavo se spremeni	Ko izdelate povezavo z dinami–Źnim klju–Źem, podate skupino dinami–Źnih klju–Źev in identifikator oddaljenega stre┼žnika klju–Źev. Ko si kasneje ogledate lastnosti povezanega povezovalnega objekta, se na strani Splo┼íno prika┼že isti identifikator oddaljenega stre┼žnika klju–Źev, toda druga skupina dinami–Źnih klju–Źev.

Sporo–Žilo o napaki VPN: TCP5B28

Simptom:
–íe poskusite aktivirati pravila za filtriranje za dolo–Źen vmesnik, se prika┼že naslednje sporo–Žilo o napaki:

TCP5B28: kr┼íitev vrstnega reda CONNECTION_DEFINITION

Mo┼żna re┼íitev:
Pravila za filtriranje, ki ste jih poskusili aktivirati, vsebujejo definicije povezav, ki uporabljajo druga–Źen vrstni red od predhodno aktiviranega niza pravil. To napako boste najpreprosteje re┼íili tako, da boste aktivirali datoteko pravil za **vse vmesnike** in ne za dolo–Źen vmesnik.

Sporo–Žilo o napaki VPN: postavka ni bila najdena

Simptom:
Ko v oknu Delo z navideznim zasebnim omre┼żjem z desno tipko mi┼íke kliknete objekt in izberete **Lastnosti** ali **Zbri┼íi**, se prika┼že naslednje sporo–Žilo:

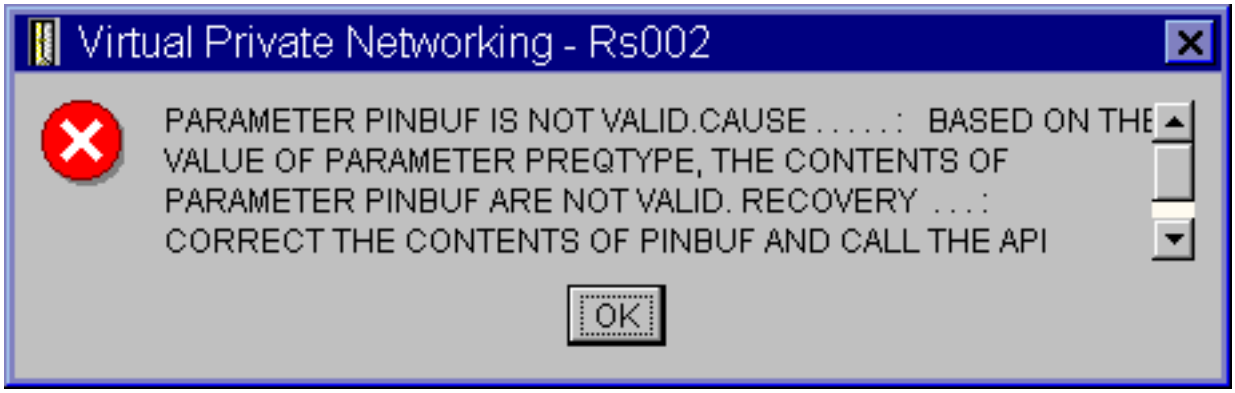
Mo┼żna re┼íitev:

- Objekt ste morda zbrisali ali preimenovali, okna pa ┼íe niste osve┼żili. Posledi–Źno je objekt ┼íe vedno prikazan v oknu Delo z navideznim zasebnim omre┼żjem. Z menija **Prikaz** izberite **Osve┼żi**, in videli boste, ali je bila te┼žava v tem. –íe je objekt ┼íe vedno prikazan v oknu Delo z navideznim zasebnim omre┼żjem, nadaljujte z naslednjim elementom tega seznama.
- Pri konfiguriranju lastnosti za objekt je morda pri┼ílo do komunikacijske napake med stre┼žnikom VPN in iSeries(TM). ┼átevilni objekti, ki so prikazani v oknu Delo z navideznim zasebnim omre┼żjem, so povezani z ve–Ź kot enim objektom v bazi podatkov na–Źel VPN. To pomeni, da lahko komunikacijske napake povzro–Žijo, da so nekateri objekti iz baze podatkov ┼íe naprej povezani z objektom v VPN. Vsaki–Ź, ko izdelate ali a┼žurirate objekt, bo v primeru dejanske izgube sinhronizacije pri┼ílo do napake. To te┼žavo lahko odpravite edino tako, da v oknu napake izberete **Potrdi**. S tem boste zagnali stran lastnosti za objekt, v katerem je pri┼ílo do napake. Na strani lastnosti ima vrednost samo polje imena, vse druge vrednosti pa so prazne (ali vsebujejo privzete vrednosti). Vnesite pravilne atribute objekta in izberite **Potrdi**, da boste shranili spremembe.

- Podobna napaka se zgodi, –Će poskusite zbrisati objekt. To te┼žavo odpravite tako, da izpolnite prazno stran lastnosti, ki se odpre, ko v sporo–Žilu o napaki kliknete **Potrdi**. S tem a┼žurirate vse izgubljene povezave z bazo podatkov na–Žel VPN. Zdaj lahko objekt zbri┼íete.

Sporo–Žilo o napaki VPN: PARAMETER PINBUF NI VELJAVEN

Simptom:
Ko poskusite zagnati povezavo, se prika┼že sporo–Žilo, podobno naslednjemu:



Mo┼żna re┼íitev:
Do te napake pride, –Će je va┼í sistem nastavljen za uporabo dolo–Ženih dr┼žavnih nastavitev, za katere se male –Źrke napa–Žno preslikajo. To napako popravite tako, da zagotovite, da vsi objekti uporabljajo samo velike –Źrke ali tako, da spremenite dr┼žavne nastavitve sistema.

Sporo–Žilo o napaki VPN: postavka ni bila najdena, oddaljen stre┼żnik klju–Žev...

Simptom:
–îe za skupino dinami–Žnega klju–Źa izberete **Lastnosti**, se prika┼že sporo–Žilo, podobno naslednjemu:

Mo┼żna re┼íitev:
Do te napake pride, –Će izdelate povezavo z dolo–Ženim identifikatorjem oddaljenega stre┼żnika klju–Žev, nato pa oddaljen stre┼żnik klju–Žev odstranite iz njegove skupine dinami–Žnih klju–Žev. To napako popravite tako, da v sporo–Žilu o napaki kliknete **Potrdi**. S tem odprete stran lastnosti za povezavo dinami–Žnega klju–Źa, v kateri je pri┼ílo do napake. Tu lahko oddaljen stre┼żnik klju–Žev vrnete nazaj v skupino dinami–Žnih klju–Žev ali izberete drug identifikator oddaljenega stre┼żnika klju–Žev. S klikom gumba **Potrdi** na strani lastnosti shranite spremembe.

Sporo–Žilo o napaki VPN: objekta ni mogo–Će a┼żurirati

Simptom:
–îe izberete na strani lastnosti za skupino dinami–Žnih klju–Žev ali ro–Žno povezavo **Potrdi**, se prika┼že naslednje sporo–Žilo:

Mo┼żna re┼íitev:
Do te napake pride, ─Če aktivna povezava uporablja objekt, ki ga posku┼íate spremeniti. Sprememb v objektu ne morete opraviti znotraj aktivne povezave. ─Še ┼żelite objekt spremeniti, dolo─Žite ustrezno aktivno povezavo, jo kliknite z desno tipko mi┼íke in s prikazanega kontekstnega menija izberite **Zaustavi**.

Sporo─Žilo o napaki VPN: klju─Ža ni mogo─Če ┼íifrirati...

Simptom:
Prika┼że se naslednje sporo─Žilo o napaki:

Mo┼żna re┼íitev:
QRETSVRSEC je sistemska vrednost, ki ka┼że, ali lahko sistem shranjuje ┼íifrirane klju─Že. ─Še je ta vrednost nastavljena na 0, potem klju─Žev z vnaprej dolo─Ženo skupno rabo in klju─Žev za algoritme v ro─Žni povezavi ni mogo─Če shraniti v bazo podatkov na─Žel VPN. Za odpravo te te┼żave uporabite v sistemu emulacijsko sejo 5250. V ukazno vrstico vpi┼íite wrksysval in pritisnite **Enter**. Na seznamu poi┼í─Žite QRETSVRSEC in poleg njega vpi┼íite 2 (spremeni). V naslednjem oknu vpi┼íite 1 in pritisnite **Enter**.

Sporo─Žilo o napaki VPN: CPF9821

Simptom:
Ko poskusite raz┼íiriti vsebnik na─Žel IP v Navigatorju iSeries(TM), se prika┼że sporo─Žilo CPF9821- Nimate pooblastila za program QTFRPRS v knji┼żnici QSYS.

Mo┼żna re┼íitev:
Morda nimate zahtevanega pooblastila za pridobitev trenutnega statusa pravil paketov ali Upravljalnika povezav VPN. Preverite, ali imate dostop do funkcije pravil paketov v Navigatorju iSeries.

Napaka VPN: Vsi klju─Ži so prazni

Simptom:
Vsi klju─Ži z vnaprej dolo─Ženo skupno rabo in klju─Ži algoritmov za ro─Žne povezave so prazni.

Mo┼żna re┼íitev:
Do te napake pride, ─Če je sistemska vrednost QRETSVRSEC nastavljena nazaj na 0. Z nastavitvijo te sistemske

vrednosti na 0 zbri┼íete vse klju─Że v bazi podatkov na─Żel VPN. To te┼żavo odpravite tako, da nastavite sistemsko vrednost nazaj na 1 in nato znova vnesete vse klju─Że. Za podrobnej┼íe informacije o tem postopku preglejte sporo─Żilo o napaki: klju─Żev ni mogo─Że ┼íifrirati.

Napaka VPN: pri uporabi pravil paketov se prika┼że prijava za drug sistem

Simptom:
Pri prvi uporabil pravil paketov se prika┼że prijavni zaslon za sistem, ki ni trenutni.

Mo┼żna re┼íitev:
Pravila paketov shranjujejo pravila za za┼í─Żito paketov v integrirani datote─Źni sistem s pomo─Źjo unikode. Dodatna prijava omogo─Ża, da pridobi iSeries(TM) Access ustrezno pretvorno tabelo za unicode. To se bo zgodilo samo enkrat.

Napaka VPN: prazen status povezave v oknu Navigatorja iSeries

Simptom:
Povezava nima v stolpcu **Status** okna Navigatorja iSeries(TM) nobene vrednosti.

Mo┼żna re┼íitev:
Prazna vrednost statusa ka┼że, da je povezava v postopku zagona. To pomeni, da se ┼íe ne izvaja, toda v njej tudi ┼íe ni pri┼ílo do napake. Ko osve┼żite okno, bo za povezavo prikazan status Napaka, Omogo─Żena, Na zahtevo ali Mirujo─Ża.

Napaka VPN: povezava ima po zaustavitvi status omogo─Żena

Simptom:
Ko zaustavite povezave, okno Navigatorja iSeries(TM) ka┼że, da je povezava ┼íe vedno omogo─Żena.

Mo┼żna re┼íitev:
Do tega obi─Źajno pride, ─Że ┼íe niste osve┼żili okna Navigatorja iSeries. Tak┼íno okno vsebuje zastarele informacije. Napako popravite tako, da z menija **Prikaz** izberete **Osve┼ži**.

Napaka VPN: 3DES ni na voljo za ┼íifriranje

Simptom:
Pri delu s pretvorbo na─Żel IKE, pretvorbo podatkovnih na─Żel ali ro─Źno povezavo, algoritem ┼íifriranja 3DES ni na voljo.

Mo┼żna re┼íitev:
Najbr┼ż imate v sistemu name┼í─Żen samo izdelek ponudnika ┼íifriranega dostopa AC2 (5722-AC2), ne pa tudi ponudnika ┼íifriranega dostopa AC3 (5722-AC3). AC2 zaradi omejitev v dol┼żinah klju─Żev omogo─Ża samo algoritem ┼íifriranja DES (Data Encryption Standard).

Napaka VPN: v oknu Navigatorja iSeries so prikazani nepri─Żakovani stolpci

Simptom:
Nastavili ste stolpce, ki jih ┼żelite prikazati v oknu Navigatorja iSeries za povezave VPN, toda ko si okno ogledate kasneje, so prikazani drugi stolpci.

Mo┼żna re┼íitev:
─îe spremenite stolpce za prikaz, spremembe niso specifi─Źne za dolo─Żenega uporabnika ali PC, pa─Ź za celoten sistem. ─îe torej nekdo drug spremeni stolpce v oknu, spremembe vplivajo na vse, ki si ogledujejo povezave v tem sistemu.

Napaka VPN: Aktivnih pravil za filtriranje ni mogo─Że deaktivirati

Simptom:
Ko poskusite deaktivirati trenutni niz pravil za filtriranje, se v oknu rezultatov prika┼że sporo─Żilo Aktivnih pravil ni mogo─Że deaktivirati.

Mo┼żna re┼íitev:
Obi─Źajno pomeni to sporo─Źilo o napaki, da obstaja vsaj ena aktivna povezava VPN. Zaustaviti morate vse povezave, ki imajo status omogo─Ćena. V ta namen z desno tipko mi┼íke kliknite vse aktivne povezave in izberite **Zaustavi**. Zdaj lahko deaktivirate pravila za filtriranje.

Napaka VPN: skupina povezav s klju─Źi za povezavo se spremeni

Simptom:
Ko izdelate povezavo z dinami─Źnim klju─Źem, podate skupino dinami─Źnih klju─Źev in identifikator oddaljenega stre┼żnika klju─Źev. ─Źe kasneje v povezanem povezovalnem objektu izberete **Lastnosti**, je na strani **Splo┼íno** strani lastnosti prikazan isti identifikator oddaljenega stre┼żnika klju─Źev, toda druga skupina dinami─Źnih klju─Źev.

Mo┼żna re┼íitev:
Identifikator je edini podatek, shranjen v bazi podatkov na─Źel VPN, ki se nana┼ía na oddaljeni stre┼żnik klju─Źev povezave z dinami─Źnim klju─Źem. Ko VPN i┼í─Źe na─Źelo za oddaljeni stre┼żnik klju─Źev, poi┼í─Źe prvo skupino dinami─Źnih klju─Źev, v kateri je identifikator oddaljenega stre┼żnika klju─Źev. Pri ogledu lastnosti za eno izmed teh povezav torej uporabi isto skupino dinami─Źnih klju─Źev, kot jo je na┼íel VPN. ─Źe ne ┼żelite povezati skupine dinami─Źnih klju─Źev z oddaljenim stre┼żnikom klju─Źev, lahko naredite nekaj od naslednjega:

1. Oddaljeni stre┼żnik klju─Źev odstranite iz skupine dinami─Źnih klju─Źev.
2. V levem podoknu vmesnika VPN raz┼íirite mo┼żnost **Po skupinah** ter izberete in povle─Źete ┼żeleno skupino dinami─Źnih klju─Źev na vrh tabele v desnem podoknu. S tem zagotovite, da bo VPN najprej pregledal to skupino dinami─Źnih klju─Źev za oddaljeni stre┼żnik klju─Źev.

Odpravljanje te┼żav v VPN z dnevnikom QIPFILTER

Dnevnik QIPFILTER je shranjen v knji┼żnici QUSRSYS in vsebuje informacije o nizih pravil za filtriranje, kot tudi informacije o tem, ali je datagram IP dovoljen ali zavrnjen. Bele┼żenje se izvaja na osnovi mo┼żnosti bele┼żenja, ki jo podate v pravilih za filtriranje.

Kako omogo─Źiti dnevnik za filter paketov IP
Dnevnik QIPFILTER aktivirajte s pomo─Źjo urejevalnika pravil paketov v Navigatorju iSeries(TM). Funkcijo bele┼żenja morate omogo─Źiti za vsako posamezno pravilo za filtriranje. Funkcija, ki bi omogo─Źala bele┼żenje za vse datagrame IP, ki prihajajo v sistem ali odhajajo iz njega, ne obstaja.

Opomba: ─Źe ┼żelite omogo─Źiti dnevnik QIPFILTER, morate deaktivirati filtre.

Naslednji koraki opisujejo, kako omogo─Źiti bele┼żenje za dolo─Źeno pravilo filtriranja:

1. V Navigatorju iSeries raz┼íirite ikono va┼íega stre┼żnika **—> Omre┼żje—> Na─Źela IP**.
2. Z desno tipko mi┼íke kliknite **Pravila paketov** in izberite **Konfiguracija**. S tem prika┼żete vmesnik pravil paketov.
3. Odprite obstoje─Źo datoteko pravil za filtriranje.
4. Dvokliknite pravilo za filtriranje, za katerega ┼żelite izvajati bele┼żenje.
5. Na strani **Splo┼íno** izberite v polju **Bele┼żenje Celotno**, tako kot v pogovornem oknu, prikazanem zgoraj. S tem omogo─Źite bele┼żenje za to dolo─Źeno pravilo filtriranja.
6. Kliknite **Potrdi**.
7. Shranite in aktivirajte spremenjeno datoteko pravil za filtriranje.

─Źe se datagram IP ujema z definicijami pravila za filtriranje, je v dnevnik QIPFILTER zabele┼żena postavka.

Kako uporabiti dnevnik QIPFILTER
Ko prvi─Ź aktivirate filtriranje paketov IP, OS/400(R) samodejno izdela dnevnik. ─Źe si ┼żelite v dnevniku ogledati podrobnosti, specifi─Źne za postavko, lahko prika┼żete postavke na zaslonu ali uporabite izhodno datoteko.

–îe prekopirate postavke dnevnika v izhodno datoteko, si jih lahko preprosto ogledate s pomo–Źjo pomo┼żnih poizvedbenih programov kot sta Query/400 ali SQL. Napi┼íete pa lahko tudi lastne programe HLL, ki obdelajo postavke v izhodnih datotekah.

Sledi zgled ukaza DSPJRN (Prika┼ži dnevnik):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mojaknji┼żnica/mojadatoteka) ENTDTALEN(*VARLEN *CALC)
```

Naslednji koraki ka┼żejo, kako prekopirate postavke dnevnika QIPFILTER v izhodno datoteko:

1. S pomo–Źjo ukaza CRTDUPOBJ (Izdelaj podvojen objekt) izdelajte kopijo sistemsko podane izhodne datoteke QSYS/QATOFIPF v uporabni┼íki knji┼żnici. Sledi zgled ukaza CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mojaknji┼żnica)
       NEWOBJ(mojadatoteka)
   ```

2. S pomo–Źjo ukaza DSPJRN (Prika┼ži dnevnik) prekopirajte postavke iz dnevnika QUSRSYS/QIPFILTER v izhodno datoteko, ki ste jo izdelali v prej┼ínjem koraku.

–îe prekopirate DSPJRN v izhodno datoteko, ki ne obstaja, jo sistem izdela za vas, toda ta datoteka ne vsebuje pravilnih opisov polj.

Opomba: Dnevnik QIPFILTER vsebuje samo postavke dovolitve ali zavrnitve pravil za filtriranje, kjer je mo┼żnost bele┼żenja nastavljena na CELOTNO. –îe na primer nastavite samo pravila za filtriranje DOVOLI, so datagrami, ki niso izrecno dovoljeni, zavrnjeni. Za te zavrnjene datagrame ni v dnevnik dodana nobena postavka. Za analizo te┼żave lahko dodate pravilo za filtriranje, ki izrecno zavrne ves drug promet in izvaja celotno bele┼żenje. V dnevniku bodo tako za vse datagrame IP, ki so zavrnjeni, zabele┼żene postavke ZAVRNI. Zaradi vpliva na zmogljivost ne priporo–Źamo, da omogo–Źite bele┼żenje za vsa pravila filtriranja. Ko preizkusite nize filtrov, omejite bele┼żenje na uporaben podniz postavk.

Tabelo, ki opisuje izhodno datoteko QIPFILTER, poi┼í–Źite v temi Polja dnevnika QIPFILTER.

Polja dnevnika QIPFILTER

Naslednja tabela opisuje polja v izhodni datoteki QIPFILTER:

Ime polja	Dol┼żina polja	┼áifra	Opis	Opombe
TFENTL	5	D	Dol┼żina postavke	
TFSEQN	10	D	Zaporedna ┼ítevilka	
TFCODE	1	N	Koda dnevnika	Vedno M
TFENTT	2	N	Tip postavke	Vedno TF
TFTIME	26	N	–îasovni ┼żig SAA	
TFJOB	10	N	Ime opravila	
TFUSER	10	N	Profil uporabnika	
TFNBR	6	D	┼átevilka opravila	
TFPGM	10	N	Ime programa	
TFRES1	51	N	Rezervirano	
TFUSPF	10	N	Uporabnik	
TFSYMN	8	N	Ime sistema	
TFRES2	20	N	Rezervirano	
TFRESA	50	N	Rezervirano	
TFLINE	10	N	Opis linije	*ALL, –Źe je TFREVT U*, prazno, –Źe je TFREVT L*, ime linije, –Źe je TFREVT L

Ime polja	Dol┼žina polja	┼áifra	Opis	Opombe
TFREVT	2	N	Dogodek pravila	L* ali L, ─Će so pravila nalo┼żena. U*, ─Će so pravila odstranjena, A pri dejanju filtra
TFPDIR	1	N	Smer paketa IP	O je izhodna, I je vhodna
TFRNUM	5	N	┼átevilka pravila	Velja za ┼ítevilko pravila v aktivni datoteki pravil
TFACT	6	N	Opravljeno dejanje filtra	DOVOLI, ZAVRNI ali IPSEC
TFPROT	4	N	Protokol prenosa	1 je ICMP 6 je TCP 17 je UDP 50 je ESP 51 je AH
TFSRCA	15	N	Izvorni naslov IP	
TFSRCP	5	N	Izvorna vrata	Odpadki, ─Će je TFPROT= 1 (ICMP)
TFDSTA	15	N	Ciljni naslov IP	
TFDSTP	5	N	Ciljna vrata	Odpadki, ─Će je TFPROT= 1 (ICMP)
TFTEXT	76	N	Dodatno besedilo	Vsebuje opis, ─Će je TFREVT= L* ali U*

Odpravljanje te┼żav v VPN z dnevnikom QVPN

VPN uporablja lo─Źen dnevnik za bele┼żenje informacij o prometu IP in povezavah, imenovan dnevnik QVPN. QVPN je shranjen v knji┼żnici QUSRSYS. Koda dnevnika je M, tipa dnevnika pa TS. Postavke dnevnika boste redkokdaj uporabljali vsak dan. Toda morda se vam bodo zdele koristne pri odpravljanju te┼żav in preverjanju, ali delujejo sistem, klju─Źi in povezave na na─Źin, ki ste ga podali. Tako vam postavke dnevnika na primer pomagajo razumeti, kaj se je zgodilo s podatkovnimi paketi in vas obve┼í─Źajo o trenutnem statusu VPN.

Kako omogo─Źiti dnevnik VPN

Dnevnik VPN aktivirajte s pomo─Źjo vmesnika za delo z navideznim zasebnim omre┼żjem v Navigatorju iSeries(TM). Funkcija, ki bi omogo─Źala bele┼żenje za vse povezave VPN, ne obstaja. Zato jo morate omogo─Źiti za vsako posamezno skupino dinami─Źnih klju─Źev ali ro─Źno povezavo.

Naslednji koraki opisujejo, kako omogo─Źiti funkcijo bele┼żenja za dolo─Źeno skupino dinami─Źnih klju─Źev ali ro─Źno povezavo:

1. V Navigatorju iSeries raz┼íirite ikono va┼íega stre┼żnika **—> Omre┼żje —> Na─Źela IP—> Delo z zasebnim navideznim omre┼żjem —> Za┼í─Źitene povezave.**
2. Za skupino dinami─Źnih klju─Źev raz┼íirite **Po skupini**, nato pa z desno tipko mi┼íke kliknite skupino dinami─Źnih klju─Źev, za katero ┼żelite omogo─Źiti bele┼żenje, in izberite **Lastnosti.**
3. Za ro─Źne povezave raz┼íirite **Vse povezave** in z desno tipko mi┼íke kliknite ro─Źno povezavo, za katero ┼żelite omogo─Źiti bele┼żenje.
4. Na strani **Bele┼żenje** izberite potrebno raven bele┼żenja. Izberete lahko med ┼ítirimi mo┼żnostmi. Te so:
   Ni─Ź
   Za to skupino povezav se ne izvaja bele┼żenje.
   Vse

Bele┼ženje se izvaja za vse dejavnosti povezav, kot sta zagon ali zastavitev povezave, ali osve┼žitve klju─Źev, kot tudi za informacije o prometu IP.

Dejavnost povezave
Bele┼ženje se izvaja za dejavnosti povezave kot sta njen zagon ali zaustavitev.

Promet IP
Bele┼ženje se izvaja za ves promet VPN, ki je povezan s to povezavo. Postavka dnevnika je zabele┼žena vsaki─Ź, ko je poklicano pravilo za filtriranje. Sistem bele┼ži informacije o prometu IP v dnevnik QIPFILTER, ki je shranjen v knji┼žnici QUSRSYS.

5. Kliknite **Potrdi**.
6. Za aktiviranje bele┼ženja za┼ženite povezavo.

Opomba: Preden lahko zaustavite bele┼ženje, morate zagotoviti, da povezava ni aktivna. ─Źe ┼želite spremeniti status bele┼ženja skupine povezav, zagotovite, da ni s to dolo─Źeno skupino povezana nobena aktivna povezava.

Kako uporabiti dnevnik VPN
─Źe si ┼želite v dnevniku VPN ogledati podrobnosti, specifi─Źne za postavko, lahko prika┼žete postavke na zaslonu ali uporabite izhodno datoteko.

─Źe prekopirate postavke dnevnika v izhodno datoteko, si jih lahko preprosto ogledate s pomo─Źjo pomo┼žnih poizvedbenih programov kot sta Query/400 ali SQL. Napi┼íete pa lahko tudi lastne programe HLL, ki obdelajo postavke v izhodnih datotekah. Sledi zgled ukaza DSPJRN (Prika┼ži dnevnik):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mojaknji┼žnica/mojadatoteka) ENTDTALEN(*VARLEN *CALC)
```

Naslednji koraki ka┼žejo, kako prekopirati postavke dnevnika VPN v izhodno datoteko:

1. Izdelajte kopijo sistemsko podane izhodne datoteke QSYS/QATOVSOF v uporabni┼íki knji┼žnici. To lahko naredite s pomo─Źjo ukaza CRTDUPOBJ (Izdelaj podvojen objekt). Sledi zgled ukaza CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mojaknji┼žnica)
       NEWOBJ(mojadatoteka)
   ```

2. S pomo─Źjo ukaza DSPJRN (Prika┼ži dnevnik) prekopirajte postavke iz dnevnika QUSRSYS/QVPN v izhodno datoteko, ki ste jo izdelali v prej┼ínjem koraku. ─Źe poskusite prekopirati DSPJRN v izhodno datoteko, ki ne obstaja, jo sistem izdela za vas, toda ta datoteka ne vsebuje pravilnih opisov polj.

Tabelo, ki opisuje polja v izhodni datoteki QVPN poi┼í─Źite v temi Polja dnevnika QVPN.

Polja dnevnika QVPN

Naslednja tabela opisuje polja v izhodni datoteki QVPN:

Ime polja	Dol┼žina polja	┼átevilsko	Opis	Opombe
TSENTL	5	D	Dol┼žina postavke	
TSSEQN	10	D	Zaporedna ┼ítevilka	
TSCODE	1	N	Koda dnevnika	Vedno M
TSENTT	2	N	Tip postavke	Vedno TS
TSTIME	26	N	─Źasovni ┼žig postavke SAA	
TSJOB	10	N	Ime opravila	
TSUSER	10	N	Uporabnik opravila	
TSNBR	6	D	┼átevilka opravila	
TSPGM	10	N	Ime programa	
TSRES1	51	N	Neuporabljen	
TSUSPF	10	N	Ime profila uporabnika	

Ime polja	Dol┼żina polja	┼átevilsko	Opis	Opombe
TSSYNM	8	N	Ime sistema	
TSRES2	20	N	Neuporabljen	
TSRESA	50	N	Neuporabljen	
TSESDL	4	D	Dol┼żina specifi─Źnih podatkov	
TSCMPN	10	N	Komponenta VPN	
TSCONM	40	N	Ime povezave	
TSCOTY	10	N	Tip povezave	
TSCOS	10	N	Stanje povezave	
TSCOSD	8	N	Za─Źetni datum	
TSCOST	6	N	Za─Źetni ─Źas	
TSCOED	8	N	Kon─Źni datum	
TSCOET	6	N	Kon─Źni ─Źas	
TSTRPR	10	N	Protokol prenosa	
TSLCAD	43	N	Naslov lokalnega odjemalca	
TSLCPR	11	N	Lokalna vrata	
TSRCAD	43	N	Naslov oddaljenega odjemalca	
TSCPR	11	N	Oddaljena vrata	
TSLEP	43	N	Lokalna zaklju─Źna to─Źka	
TSREP	43	N	Oddaljena zaklju─Źna to─Źka	
TSCORF	6	N	┼átevilo osve┼żitev	
TSRFDA	8	N	Datum naslednje osve┼żitve	
TSRFTI	6	N	─Źas naslednje osve┼żitve	
TSRFLS	8	N	Trajanje osve┼żitve	
TSSAPH	1	N	Faza SA	
TSAUTH	10	N	Tip overjanja	
TSENCR	10	N	Tip ┼íifriranja	
TSDHGR	2	N	Skupina Diffie-Hellman	
TSERRC	8	N	Koda napake	

Odpravljanje te┼żav v VPN z dnevniki opravil VPN

─Źe imate te┼żave s povezavami VPN, je vedno priporo─Źljivo analizirati dnevnike opravil. Obstaja veliko dnevnikov opravil, ki vsebujejo sporo─Źila o napakah in druge informacije, povezane z okoljem VPN.

Pomembno je, da analizirate dnevnik opravil na obeh straneh povezave, ─Że sta obe strani stre┼żnika iSeries(TM). ─Źe ni mogo─Że zagnati dinami─Źne povezave, vam bo pomagalo, ─Że boste razumeli, kaj se dogaja v oddaljenem sistemu.

Opravili VPN QTOVMAN in QTOKVPNIKE se izvajata v podsistemu QSYSWRK. Njuna ustrezna dnevnika opravil si lahko ogledate v Navigatorju iSeries OS/400(R).

V tem razdelku bomo predstavili najpomembnej┼ía opravila za okolje VPN. Naslednji seznam navaja imena opravil, ki jim sledi kratka razlaga namena opravila:

QTCPIP
To opravilo je osnovno opravil, ki za┼žene vse vmesnike TCP/IP. Dnevnik opravil QTCPIP analizirajte, ─Če imate splo┼íne osnovne te┼žave s TCP/IP.

QTOKVPNIKE
Opravilo QTOKVPNIKE je opravilo Upravljalnika klju─Ćev VPN. Upravljalnik klju─Ćev VPN poslu┼ía na vratih UDP 500, kjer izvaja obdelavo protokola IKE (Internet Key Exchange.

QTOVMAN
To opravilo je Upravljalnik povezav za povezave VPN. Povezan dnevnik opravil vsebuje sporo─Ćila za vsak neuspel poskus povezave.

QTPPANSxxx
To opravilo se uporablja za klicne povezave PPP. Odgovarja na poskuse povezav, za katere je v profilu PPP definiran *ANS.

QTPPPCTL
To je opravilo PPP za klicanje iz omre┼żja.

QTPPPL2TP
To je opravilo upravljalnika L2TP (Layer Two Tunneling Protocol). Sporo─Ćila v tem dnevniku opravil preglejte, ─Če imate te┼žave z nastavitvijo tunela L2TP.

Splo┼ína sporo─Ćila o napakah Upravljalnika povezav VPN
Razdelek opisuje nekaj najpogostej┼íih sporo─Ćil o napakah Upravljalnika povezav VPN, na katere lahko naletite.

Na splo┼íno zabele┼żi Upravljalnik povezav VPN v primeru napake v povezavi VPN v dnevnik opravil QTOVMAN dve sporo─Ćili. Prvo sporo─Ćilo nudi podrobnosti o napaki. Informacije o teh napakah si lahko ogledate v Navigatorju iSeries(TM), tako da z desno tipko mi┼íke kliknete povezavo, v kateri je pri┼ílo do napake, in izberete **Informacije o napaki**.

Drugo sporo─Ćilo opisuje dejanje, ki ste ga poskusili izvesti v povezavi, ko je pri┼ílo do napake, kot je na primer zagon ali zaustavitev povezave. Sporo─Ćila TCP8601, TCP8602 in TCP860A, opisana spodaj, so zna─Ćilni zgledi drugih sporo─Ćil.

Sporo─Ćila o napakah Upravljalnika povezav VPN

Sporo─Ćilo	Vzrok	Dejanje
TCP8601 Povezave VPN [*ime povezave*] ni bilo mogo─Će zagnati.	Te povezave VPN ni bilo mogo─Će zagnati zaradi ene izmed naslednjih kod vzroka: *0* - Prej┼ínje sporo─Ćilo v dnevniku opravil z istim imenom povezave VPN vsebuje podrobnej┼íe informacije. *1* - Konfiguracija na─Ćela VPN. *2* - Napaka v omre┼żnih komunikacijah. *3* - Upravljalnik klju─Ćev VPN ni uspel dogovoriti novega dogovora za za┼í─Ćito. *4* - Oddaljena zaklju─Ćna to─Ćka za to povezavo ni pravilno konfigurirana. *5* - Upravljalnik klju─Ćev VPN ni uspel odgovoriti Upravljalniku povezav VPN. *6* - Napaka pri nalaganju povezave VPN za komponento za┼í─Ćite IP. *7* - Napaka v komponenti PPP.	1. Dodatna sporo─Ćila poi┼í─Ćite v dnevnikih opravil. 2. Popravite napake in ponovite zahtevo. 3. S pomo─Ćjo Navigatorja iSeries si oglejte status povezave. Povezave, ki jih ni mogo─Će zagnati, bodo imele status napake.

Sporo─Žilo	Vzrok	Dejanje
TCP8602 Napaka se je zgodila pri zaustavitvi povezave VPN [*ime povezave*].	Zahtevali ste zaustavitev podane povezave VPN, toda povezava se ni zaustavila ali pa se je zaradi ene izmed naslednjih kod vzroka zaustavila z napako: *0* - Prej┼ínje sporo─Žilo v dnevniku opravil z istim imenom povezave VPN vsebuje podrobnej┼íe informacije. *1* - Povezava VPN ne obstaja. *2* - Notranja komunikacijska napaka v Upravljalniku klju─Źev VPN. *3* - Notranja komunikacijska napaka v komponenti IPSec. *4* - Komunikacijska napaka v oddaljeni zaklju─Źni to─Źki povezave VPN.	1. Dodatna sporo─Žila poi┼í─Žite v dnevnikih opravil. 2. Popravite napake in ponovite zahtevo. 3. S pomo─Źjo Navigatorja iSeries si oglejte status povezave. Povezave, ki jih ni mogo─Že zagnati, bodo imele status napake.
TCP8604 Zagon povezave VPN [*ime povezave*] ni uspel.	Zagon te povezave VPN ni uspel zaradi ene izmed naslednjih kod vzroka: *1* - Imena oddaljenega gostitelja ni bilo mogo─Že prevesti v naslov IP. *2* - Imena lokalnega gostitelja ni bilo mogo─Že prevesti v naslov IP. *3* - Pravila za filtriranje na─Žela VPN, povezana s to povezavo VPN, niso nalo┼żena. *4* - Uporabni┼íko podana vrednost klju─Ża ni veljavna za ta povezani algoritem. *5* - Iniciacijska vrednost za povezavo VPN ne dopu┼í─Ża podanega dejanja. *6* - Vloga sistema za povezavo VPN ni skladna z informacijami iz povezovalne skupine. *7* - Rezervirano. *8* - Podatkovne zaklju─Źne to─Źke (lokalni in oddaljeni naslovi in storitve) te povezave VPN niso skladne z informacijami iz povezovalne skupine. *9* - Vrsta identifikatorja ni veljavna.	1. Dodatna sporo─Žila poi┼í─Žite v dnevnikih opravil. 2. Popravite napake in ponovite zahtevo. 3. Konfiguracijo na─Žel VPN lahko preverite ali popravite s pomo─Źjo Navigatorja iSeries. Preverite, ali ima skupina dinami─Źnih klju─Źev, ki je povezana s to povezavo, konfigurirane sprejemljive vrednosti.
TCP8605 Upravljalnik povezav VPN ne more komunicirati z Upravljalnikom klju─Źev VPN.	Upravljalnik povezav VPN zahteva za vzpostavitev dogovorov za za┼í─Žito za dinami─Źne povezave VPN storitve Upravljalnika klju─Źev VPN. Upravljalnik klju─Źev VPN ni mogel komunicirati z Upravljalnikom klju─Źev VPN.	1. Dodatna sporo─Žila poi┼í─Žite v dnevnikih opravil. 2. Preverite, ali je vmesnik *LOOPBACK aktiven; v ta namen uporabite ukaz NETSTAT OPTION(*IFC). 3. Stre┼żnik VPN zaustavite z ukazom ENDTCPSVR SERVER(*VPN), nato pa ga znova za┼żenite z ukazom STRTCPSRV SERVER(*VPN). **Opomba:** To povzro─Źi zaustavitev vseh trenutnih povezav VPN.

Sporo–Žilo	Vzrok	Dejanje
TCP8606 Upravljalnik klju–Žev VPN ni uspel vzpostaviti zahtevanega dogovora za za┼í–Žito za povezavo [*ime povezave*].	Upravljalnik klju–Žev VPN ni uspel vzpostaviti zahtevanega dogovora za za┼í–Žito zaradi ene izmed naslednjih kod vzroka: *24* - Overjanje povezave Upravljalnika klju–Žev VPN ni uspelo. *8300* - Do napake je pri┼ílo med pogajanji za klju–Žno povezavo Upravljalnika klju–Žev VPN. *8306* - Lokalni klju–Ž z vnaprej dolo–Ženo skupno rabo ni bil najden. *8307* - Oddaljeno na–Želo faze 1 IKE ni bilo najdeno. *8308* - Oddaljen klju–Ž z vnaprej dolo–Ženo skupno rabo ni bil najden. *8327* - Pogajanja za klju–Žno povezavo Upravljalnika klju–Žev VPN so bila prekinjena. *8400* - Do napake je pri┼ílo med pogajanji za povezavo VPN Upravljalnika klju–Žev VPN. *8407* - Oddaljeno na–Želo faze 2 IKE ni bilo najdeno. *8408* - Pogajanja za povezavo VPN Upravljalnika klju–Žev VPN so bila prekinjena. *8500 ali 8509* - Zgodila se je omre┼żna napaka Upravljalnika klju–Žev VPN.	1. Dodatna sporo–Žila poi┼í–Žite v dnevnikih opravil. 2. Popravite napake in ponovite zahtevo. 3. Konfiguracijo na–Žel VPN lahko preverite ali popravite s pomo–Žjo Navigatorja iSeries. Preverite, ali ima skupina dinami–Žnih klju–Žev, ki je povezana s to povezavo, konfigurirane sprejemljive vrednosti.
TCP8608 Povezava VPN [*ime povezave*] ni mogla pridobiti naslova NAT.	Ta skupina dinami–Žnih klju–Žev ali podatkovna povezava je podala, naj bo izveden prevod omre┼żnega naslova (NAT) za enega ali ve–Ž naslovov, toda ta ni bil izveden zaradi ene izmed naslednjih kod vzroka: *1* - Naslov, za katerega ┼żelite uveljaviti NAT, ni samostojen naslov IP. *2* - Vsi razpolo┼żljivi naslovi so bili uporabljeni.	1. Dodatna sporo–Žila poi┼í–Žite v dnevnikih opravil. 2. Popravite napake in ponovite zahtevo. 3. Na–Želo VPN lahko preverite ali popravite s pomo–Žjo Navigatorja iSeries. Preverite, ali ima skupina dinami–Žnih klju–Žev, ki je povezana s to povezavo, konfigurirane sprejemljive vrednosti za naslove.
TCP8620 Lokalna zaklju–Žna to–Žka povezave ni na voljo.	Teh povezav VPN ni bilo mogo–Že omogo–Žiti, ker lokalna zaklju–Žna to–Žka povezave ni bila na voljo.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. Preverite, ali je lokalna zaklju–Žna to–Žka povezave definirana in zagnana; v ta namen uporabite ukaz NETSTAT OPTION(*IFC). 3. Popravite napake in ponovite zahtevo.
TCP8621 Lokalna zaklju–Žna podatkovna to–Žka ni na voljo.	Te povezave VPN ni bilo mogo–Že omogo–Žiti, ker lokalna zaklju–Žna podatkovna to–Žka ni bila na voljo.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. Preverite, ali je lokalna zaklju–Žna to–Žka povezave definirana in zagnana; v ta namen uporabite ukaz NETSTAT OPTION(*IFC). 3. Popravite napake in ponovite zahtevo.

Sporo–Žilo	Vzrok	Dejanje
TCP8622 Enkapsulacija prenosa ni dovoljena s prehodom.	Te povezave VPN ni bilo mogo–Že omogo–Žiti, ker dogovorjeno na–Želo podaja na–Žin enkapsulacije prenosa, ta povezava pa je definirana kot za┼í–Žitni prehod.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. Za spreminjanje na–Žela VPN, povezanega s to povezavo VPN, uporabite Navigator iSeries. 3. Popravite napake in ponovite zahtevo.
TCP8623 Povezava VPN se prekriva z obstoje–Žo povezavo.	Te povezave VPN ni bilo mogo–Že omogo–Žiti, ker je obstoje–Ža povezava VPN ┼že omogo–Žena. Lokalna zaklju–Žna podatkovna to–Žka te povezave je [*vrednost lokalne podatkovne zaklju–Žne to–Žke*], oddaljena zaklju–Žna podatkovna to–Žka pa [*vrednost oddaljene zaklju–Žne podatkovne to–Žke*].	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries si oglejte vse omogo–Žene povezave, katerih lokalne podatkovne zaklju–Žne to–Žke in oddaljene podatkovne zaklju–Žne to–Žke prekrivajo povezavo. –Če sta zahtevani obe povezavi, spremenite na–Želo obstoje–Že povezave. 3. Popravite napake in ponovite zahtevo.
TCP8624 Povezava VPN ni v obmo–Žju povezanega pravila za filtriranje na–Žela.	Te povezave VPN ni bilo mogo–Že omogo–Žiti, ker podatkovne zaklju–Žne to–Žke niso znotraj definiranega pravila za filtriranje na–Žela.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries prika┼żite omejitve podatkovne zaklju–Žne to–Žke za to povezavo ali skupino dinami–Žnih klju–Žev. –Če je izbrana mo┼żnost **Podniz filtra na–Žel** ali **Prilagodi, tako da se ujema s filtrom na–Žel**, preverite podatkovne zaklju–Žne to–Žke povezave. Te morajo ustrezati aktivnemu pravilu za filtriranje, ki ima dejanje IPSEC in ime povezave VPN, ki je povezano s to povezavo. Spremenite na–Želo obstoje–Že povezave ali pravilo za filtriranje, da boste omogo–Žili to povezavo. 3. Popravite napake in ponovite zahtevo.
TCP8625 Povezava VPN ni prestala preverjanja algoritma ESP.	Te povezave VPN ni bilo mogo–Že omogo–Žiti, ker tajni klju–Ž, povezan s to povezavo, ni bil zadosten.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries prika┼żite na–Želo, povezano s to povezavo, in vnesite drug tajni klju–Ž. 3. Popravite napake in ponovite zahtevo.

Sporo–Žilo	Vzrok	Dejanje
TCP8626 Zaklju–Žna to–Žka povezave VPN ni ista kot podatkovna zaklju–Žna to–Žka.	Te povezave VPN ni bilo mogo–Že vzpostaviti, ker na–Želo podaja, da je gostitelj, toda zaklju–Žna to–Žka povezave VPN ni ista kot podatkovna zaklju–Žna to–Žka.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries prika┼žite omejitve podatkovne zaklju–Žne to–Žke za to povezavo ali skupino dinami–Žnih klju–Žev. –če je izbrana mo┼žnost **Podniz filtra na–Žel** ali **Prilagodi, tako da se ujema s filtrom na–Žel**, preverite podatkovne zaklju–Žne to–Žke povezave. Te morajo ustrezati aktivnemu pravilu za filtriranje, ki ima dejanje IPSEC in ime povezave VPN, ki je povezano s to povezavo. Spremenite na–Želo obstoje–Že povezave ali pravilo za filtriranje, da boste omogo–Žili to povezavo. 3. Popravite napake in ponovite zahtevo.
TCP8628 Pravila za filtriranje na–Žel niso nalo┼žena.	Pravilo za filtriranje na–Žel za to povezavo ni aktivno.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries prika┼žite aktivne filtre na–Žel. Preverite pravilo za filtriranje na–Žel za to povezavo. 3. Popravite napake in ponovite zahtevo.
TCP8629 Paket IP za povezavo VPN je bil zbrisan.	Ta povezava VPN ima konfiguriran VPN NAT, toda zahtevan niz naslovov NAT je presegel razpolo┼žljive naslove NAT.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. S pomo–Žjo Navigatorja iSeries pove–Žajte ┼ítevilo naslovov NAT, ki so dodeljeni za to povezavo VPN. 3. Popravite napake in ponovite zahtevo.
TCP862A Povezave PPP ni bilo mogo–Že zagnati.	Ta povezava VPN je bila povezana s profilom PPP. Pri njenem zagonu je pri┼ílo do poskusa zagona profila PPP, toda pri┼ílo je do napake.	1. Dodatna sporo–Žila, ki se nana┼íajo na to povezavo, poi┼í–Žite v dnevnikih opravil. 2. Preglejte dnevnik opravil, ki je povezan s povezavo PPP. 3. Popravite napake in ponovite zahtevo.

Odpravljanje te┼žav v VPN s komunikacijskim sledenjem OS/400

iSeries(TM) OS/400(R) nudi zmo┼žnost za sledenje podatkov v komunikacijski linije kot je na primer vmesnik lokalnega omre┼žja (LAN) ali javnega omre┼žja (WAN). Povpre–Žen uporabnik najbr┼ž ne bo razumel celotne vsebine podatkov sledenja. Toda s pomo–Žjo postavk sledenja lahko dolo–Žite, ali je pri┼ílo do izmenjave podatkov med lokalnimi in oddaljenimi sistemi.

Zagon komunikacijskega sledenja

Komunikacijsko sledenje v sistemu za┼ženite s pomo–Žjo ukaza STRCMNTRC (Za┼żeni komunikacijsko sledenje). Sledi zgled ukaza STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('Te┼žave VPN')
```

Ukazni parametri so razlo┼żeni na naslednjem seznamu:

CFGOBJ (konfiguracijski objekt)
Ime konfiguracijskega objekta, ki mu ┼żelite slediti. Objekt je opis linije, opis omre┼żnega vmesnika ali opis omre┼żnega stre┼żnika.

CFGTYPE (tip konfiguracije)
Podaja, ali se izvaja sledenje za linijo (*LIN), omre┼żni vmesnik (*NWI) ali omre┼żni stre┼żnik (*NWS).

MAXSTG (velikost vmesnega pomnilnika)
Velikost vmesnega pomnilnika za sledenje. Privzeta vrednost je nastavljena na 128 kb. Obmo─Źje je od 128 kb do 64 Mb. Dejanska najve─Źja dovoljena velikost vmesnega pomnilnika za sistem je definirana znotraj sistemskih storitvenih orodij (SST). Zato se lahko v primeru, da uporabite v ukazu STRCMNTRC ve─Źjo velikost vmesnega pomnilnika, kot je definirana v SST, prika┼że sporo─Żilo o napaki. Ne pozabite, da ne sme vsota velikosti za vmesni pomnilnik, podana v vseh zagnanih komunikacijskih sledenjih, prese─Źi najve─Źje velikosti vmesnega pomnilnika, definirane v SST.

DTADIR (smer podatkov)
Smer prometa podatkov, ki jim sledite. Smer je lahko *SND (samo izhodni promet), *RCV (samo vhodni promet) ali *BOTH (oboje).

TRCFULL (polno sledenje)
Kaj se zgodi, ko se vmesni pomnilnik sledenja napolni. Ta parameter ima dve mo┼żni vrednosti. Privzeta vrednost je *WRAP, ki pomeni, da se za─Źne vmesni pomnilnik prepisovati. Novi zapisi med zbiranjem za─Źno prepisovati stare.

Druga vrednost *STOPTRC ustavi sledenje, ko je dose┼żeno ┼ítevilo podatkov sledenja, ki je podano v parametru MAXSTG. Na splo┼íno pazite, da boste vedno definirali velikost vmesnega pomnilnika tako, da bo dovolj velika za shranitev vseh zapisov sledenja. ─Źe se za─Źne sledenje prepisovati, lahko izgubite pomembne informacije sledenja. ─Źe imate te┼żave zaradi velikih prekinitev, definirajte vmesni pomnilnik tako, da bo dovolj velik, da s prepisovanjem ne boste zavrgli pomembnih informacij.

USRDTA (┼ítevilo uporabni┼íkih bajtov za sledenje)
Definira ┼ítevilo podatkov, za katere se bo izvajalo sledenje v uporabni┼íkem podatkovnem delu okvirjev sledenja. Po privzetku je za vmesnike LAN zajetih samo prvih 100 bajtov uporabni┼íkih podatkov. Za vse druge vmesnike so zajeti vsi uporabni┼íki podatki. ─Źe sumite na te┼żave v uporabni┼íkih podatkih okvirja, podajte *MAX.

TEXT (opis sledenja)
Nudi pomemben opis sledenja.

Zaustavitev komunikacijskega sledenja
─Źe ne podate druga─Że, se sledenje obi─Żajno zaustavi, ko pride do stanja, za katerega izvajate sledenje. Za zaustavitev sledenja uporabite ukaz ENDCMNTRC (Zaustavi komunikacijsko sledenje). Sledi zgled ukaza ENDCMNTRC:

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

Ukaz ima dva parametra:

CFGOBJ (konfiguracijski objekt)
Ime konfiguracijskega objekta, za katerega izvajate sledenje. Objekt je opis linije, opis omre┼żnega vmesnika ali opis omre┼żnega stre┼żnika.

CFGTYPE (tip konfiguracije)
Podaja, ali se izvaja sledenje za linijo (*LIN), omre┼żni vmesnik (*NWI) ali omre┼żni stre┼żnik (*NWS).

Natis podatkov sledenja
Ko zaustavite komunikacijsko sledenje, morate natisniti podatke sledenja. V ta namen uporabite ukaz PRTCMNTRC (Natisni komunikacijsko sledenje). Ker je ves promet linije zajet v ─Źasu sledenja, imate za izdelavo izhodnih podatkov na voljo ve─Ź mo┼żnosti filtriranja. Poskusite ohraniti vmesno datoteko ─Źim manj┼ío, saj bo analiza na ta na─Źin hitrej┼ía in u─Źinkovitej┼ía. V primeru te┼żave VPN filtrirajte samo promet IP in ─Że je mogo─Że na dolo─Ženem naslovu IP. Na voljo je tudi mo┼żnost filtriranja na dolo─Ženi ┼ítevilki vrat IP. Sledi zgled ukaza PRTCMNTRC:

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

V tem zgledu je sledenje formatirano samo za promet IP in vsebuje samo podatke za naslov IP, kjer je izvorni ali ciljni naslov 10.50.21.1, ┼ítevilka izvornih ali ciljnih vrat pa 500.

Spodaj smo razlo┼żili samo najpomembnej┼íe ukazne parametre za analiziranje te┼żav VPN:

CFGOBJ (konfiguracijski objekt)
Ime konfiguracijskega objekta, za katerega izvajate sledenje. Objekt je opis linije, opis omre┼żnega vmesnika ali opis omre┼żnega stre┼żnika.

CFGTYPE (tip konfiguracije)
Podaja, ali se izvaja sledenje za linijo (*LIN), omre┼żni vmesnik (*NWI) ali omre┼żni stre┼żnik (*NWS).

FMTTCP (formatiraj podatke TCP/IP)
Ali ┼żelite formatirati sledenje za podatke TCP/IP in UDP/IP. ─če ┼żelite formatirati sledenje za podatke IP, podajte *YES.

TCPIPADR (formatiraj podatke TCP/IP po naslovu)
Parameter je sestavljen iz dveh elementov. ─če podate v obeh elementih naslove IP, boste natisnili samo promet IP med temi naslovi.

SLTPORT (┼ítevilka vrat IP)
┼átevilka vrat IP, ki jo ┼żelite filtrirati.

FMTBCD (formatiraj podatke razpo┼íiljanja)
Ali ┼żelite natisniti vse okvirje razpo┼íiljanja. Privzeta vrednost je Da. ─če na primer ne ┼żelite zahtev ARP (Address Resolution Protocol), podajte *NO, sicer vas lahko popolnoma preplavijo sporo─Žila razpo┼íiljanja na vse naslove.

Povezane informacije za VPN

Dodatne scenarije in opise konfiguracije VPN poi┼í─Žite v drugih virih informacij:

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

  V tej IBM-ovi rde─Źi knjigi boste na┼íli postopek, ki po korakih opisuje konfiguriranje tunela VPN s pomo─Źjo VPN V5R1 in vgrajene podpore Windows 2000 za L2TP in IPSec.
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

Rde─Źa knjiga razlaga koncepte VPN in opisuje njegovo izvedbo s pomo─Źjo IPSec (IP security) in L2TP (Layer 2 Tunneling Protocol) v OS/400.

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

  Rde─Źa knjiga razlaga vse vgrajene funkcije omre┼żne za┼í─Źite, ki so na voljo v sistemu OS/400, kot so filtri IP, NAT, VPN, stre┼żnik proxy HTTP, SSL, DNS, podajanje po┼íte, nadzorovanje in bele┼żenje. Njihovo uporabo opi┼íe s pomo─Źjo prakti─Źnih zgledov.
- **Virtual Private Networking: Securing Connections**

  Na tej spletni strani boste na┼íli najnovej┼íe novice o VPN, najnovej┼íe PTF-je in povezave z drugimi zanimivimi spletnimi stranmi.
- **Drugi povezani priro─Źniki in rde─Że knjige o za┼í─Źiti**
  Tu si lahko ogledate neposredni seznam informacij, povezanih z za┼í─Źito.

PDF shranite na delovno postajo, kjer si ga lahko ogledate ali natisnete, takole:

1. Z desno tipko mi┼íke kliknite PDF v brskalniku (z desno tipko mi┼íke kliknite zgornjo povezavo).
2. Kliknite **Save Target As...**.
3. Izberite imenik, v katerega ┼żelite shraniti razli─Źico PDF.
4. Kliknite **Save**.

─ie potrebujete za prikaz ali ogled datotek PDF program Adobe Acrobat Reader, ga lahko presnamete na spletni strani podjetja Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Dodatek. Opombe

Te informacije smo razvili za izdelke in storitve, ki jih ponujamo v Zdru┼ženih dr┼žavah Amerike.

IBM morda teh izdelkov, storitev ali funkcij, omenjenih v tem dokumentu, ne bo nudil v drugih dr┼žavah. Informacije o izdelkih in storitvah, ki so trenutno na voljo v va┼íi dr┼žavi, boste dobili pri lokalnem IBM-ovem predstavniku. Nobena referenca na IBM-ov izdelek, program ali storitev ne trdi ali pomeni, da lahko uporabite samo ta IBM-ov izdelek, program ali storitev. Namesto njih lahko uporabite katerikoli funkcionalno enakovreden izdelek, program ali storitev, ki ne kr┼íi IBM-ovih pravic do intelektualne lastnine. Vendar pa mora uporabnik sam oceniti in preveriti delovanje vseh izdelkov, programov ali storitev, ki niso IBM-ovi.

IBM ima lahko patente ali vlo┼žene zahtevke za patente, ki pokrivajo vsebino tega dokumenta. Posedovanje tega dokumenta vam ne daje licence za te patente. Vpra┼íanja o licencah lahko po┼íljete v pisni obliki na naslednji naslov:

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

Vpra┼íanja v zvezi z licencami za DBCS naslovite na IBM-ov oddelek za intelektualno lastnino v va┼íi dr┼žavi ali po┼íljite poizvedbe v pisni obliki na naslov:

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

Naslednji odstavek ne velja za Veliko Britanijo ali druge dr┼žave, v katerih te dolo─Źbe niso v skladu z lokalnim zakonom: INTERNATIONAL BUSINESS MACHINES CORPORATION NUDI TO APLIKACIJO ″TAK┼áNO KOT JE″, BREZ JAMSTEV KAKR┼áNEKOLI VRSTE, PA NAJ BODO IZRECNA ALI POSREDNA, KAR VKLJU─îUJE, VENDAR NI OMEJENO NA POSREDNA JAMSTVA NEKR┼áITVE, TR┼ŻNOSTI ALI PRIMERNOSTI ZA DOLO─îEN NAMEN. V nekaterih dr┼žavah ni dovoljena zavrnitev izrecnih ali posrednih jamstev v dolo─Źenih transakcijah, zato ta izjava morda za vas ne velja.

Te informacije lahko vsebujejo tehni─Źne nepravilnosti ali tipografske napake. Informacije v tem dokumentu ob─Źasno spremenimo. Te spremembe bomo vklju─Żili v nove izdaje publikacije. IBM lahko kadarkoli izbolj┼ía in/ali spremeni izdelek(ke) in/ali program(e), opisane v tej publikacije brez vnaprej┼ínjega opozorila.

Vse reference v teh informacijah na spletne strani, ki niso IBM-ove, so podane zgolj zaradi priro─Źnosti, in na noben na─Źin ne pomenijo, da uporabo teh spletnih strani odobravamo. Gradivo na teh spletnih straneh ni del gradiva za ta IBM-ov izdelek in te spletne strani uporabljate na lastno odgovornost.

IBM lahko uporabi ali razdeli informacije, ki nam jih po┼íljete, na kakr┼íenkoli na─Źin, ki se mu zdi primeren, brez vsake odgovornosti do vas.

Imetniki licenc za ta program, ki potrebujejo informacije, da bi omogo─Żili: (i) izmenjavo informacij med neodvisno izdelanimi programi in drugimi programi (vklju─Żno s tem) in (ii) medsebojno uporabo informacij, ki so bile izmenjane, naj po┼íljejo vpra┼íanja na naslednji naslov:

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

Tak┼íne informacije bodo na voljo v skladu z ustreznimi dolo─Źbami in pogoji, ki lahko v dolo─Ženih primerih zajemajo tudi pla─Žilo.

Licen─Źni program, opisan v teh informacijah, in vse licen─Źno gradivo, ki je na voljo zanj, nudi IBM v skladu s pogoji IBM-ove pogodbe s strankami, IBM-ove mednarodne licen─Źne pogodbe za programe ali katerekoli enakovredne pogodbe med nami.

Vsi podatki o zmogljivosti, vsebovani tukaj, so bili dolo─Ženi v nadzorovanem okolju, zato se lahko rezultati, dobljeni v drugih operacijskih okoljih, zelo razlikujejo. Nekatere meritve so bile opravljene v sistemih na razvojni stopnji in zato ne dajemo nobenega jamstva, da bodo te meritve enake tudi v splo┼íno razpolo┼żljivih sistemih. Prav tako so bile morda nekatere meritve ocenjene z ekstrapolacijo. Dejanski rezultati se lahko razlikujejo. Uporabniki tega dokumenta naj preverijo ustrezne podatke za njihovo okolje.

Informacije, ki se nana┼íajo na izdelke drugih proizvajalcev, smo pridobili pri njihovih dobaviteljih, v njihovih objavah ali v drugih javno razpolo┼żljivih virih. Pri IBM-u teh izdelkov nismo preverili, zato ne moremo potrditi natan─Źnosti zmogljivosti, zdru┼żljivosti ali drugih zahtev, povezanih z izdelki drugih proizvajalcev. Vpra┼íanja v zvezi z zmogljivostjo izdelkov drugih proizvajalcev naslovite na dobavitelje teh izdelkov.

Vse izjave v zvezi z IBM-ovo bodo─Źo usmeritvijo ali namenom lahko spremenimo ali umaknemo brez vsakega opozorila, in predstavljajo samo cilje in namene.

Vse prikazane IBM-ove cene so IBM-ove predlagane maloprodajne cene, so trenutne in se lahko spremenijo brez obvestila. Cene se zastopnike se razlikujejo.

Te informacije so namenjene samo na─Źrtovanju. Tukaj prikazane informacije se lahko spremenijo, ┼íe preden so opisani izdelki na voljo.

Te informacije vsebujejo zglede podatkov in poro─Źil, uporabljenih v vsakodnevnih poslovnih operacijah. Da bi bili zgledi ─Źim bolj nazorni, vklju─Źujejo imena posameznikov, podjetij, znamk in izdelkov. Vsa ta imena so izmi┼íljena; vsaka podobnost z imeni in naslovi dejanskih poslovnih podjetij je zgolj naklju─Źna.

Blagovne znamke

Naslednji izrazi so blagovne znamke podjetja International Business Machines Corporation v Zdru┼żenih dr┼żavah Amerike, v drugih dr┼żavah ali oboje.
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance in WordPro so blagovne znamke International Business Machines Corporation in Lotus Development Corporation v Zdru┼żenih dr┼żavah Amerike, v drugih dr┼żavah ali oboje.

C-bus je blagovna znamka Corollary, Inc. v Zdru┼żenih dr┼żavah Amerike, ostalih dr┼żavah ali oboje.

ActionMedia, LANDesk, MMX, Pentium in ProShare so blagovne znamke ali registrirane blagovne znamke Intel Corporation v Zdru┼żenih dr┼żavah Amerike ali oboje.

Microsoft, Windows, Windows NT in logotip Windows so blagovne znamke dru┼żbe Microsoft Corporation v Zdru┼żenih dr┼żavah Amerike, v drugih dr┼żavah ali oboje.

SET in logotip SET sta blagovni znamki SET Secure Electronic Transaction LLC.

Java in vse na Javi temelje─Źe blagovne znamke so blagovne znamke podjetja Sun Microsystems, Inc. v Zdru┼żenih dr┼żavah Amerike, v drugih dr┼żavah ali oboje.

UNIX je registrirana blagovna znamka The Open Group v Zdru┼żenih dr┼żavah Amerike in ostalih dr┼żavah.

Druga imena podjetij, izdelkov ali storitev so lahko blagovne ali storitvene znamke njihovih ustreznih lastnikov.

Dolo─Źbe in pogoji za snemanje publikacij z oddaljenega ra─Źunalnika in njihov natis

Pravice za uporabo publikacij, ki ste jih izbrali za presnetje z oddaljenega ra─Źunalnika, so predmet naslednjih dolo─Źb in pogojev in va┼íe navedbe, da jih sprejmete.

Osebna uporaba: te publikacije lahko ponatisnete za svojo osebno in nekomercialno uporabo, pod pogojem, da ohranite vse oznake o lastni┼ítvu. Izpeljanih delov teh publikacij ali kateregakoli njihovega dela ne smete razdeljevati, prikazovati ali izdelovati brez izrecne privolitve IBM-a.

Komercialna uporaba: te publikacije lahko ponatisnete, razdelite in prikazujete izklju─Źno znotraj podjetja in pod pogojem, da ohranite vse oznake o lastni┼ítvu. Izdelava izpeljanih del teh publikacij ni dovoljena, ponatis, razdeljevanje ali prikazovanje teh publikacij ali kateregakoli njihovega dela izven podjetja pa ni dovoljeno brez izrecne privolitve IBM-a.

Razen kot je izrecno odobreno v tem dovoljenju, niso dodeljene nobene druge pravice, licence ali pravice, pa naj bodo izrecne ali posredne, za publikacije ali katerekoli informacije, podatke, programsko opremo ali drugo intelektualno lastnino, vsebovano v njih.

IBM si pridr┼żuje pravico umakniti dovoljenja, vsebovana v tem dokumentu, ─Źe presodi, da mu uporaba publikacij ┼íkodi ali ─Źe dolo─Źi, da zgornja navodila niso pravilno upo┼ítevana.

Te informacije lahko presnamete z oddaljenega ra─Źunalnika, jih izvozite ali na novo izvozite samo s popolnim upo┼ítevanjem vseh ustreznih zakonov in predpisov, vklju─Źno z vsemi zakoni in predpisi Zdru┼żenih dr┼żav Amerike o izvozu. IBM NE DAJE NOBENEGA JAMSTVA ZA VSEBINO TEH PUBLIKACIJ. PUBLIKACIJE SO NA VOLJO ″TAK┼áNE KOT SO″ BREZ JAMSTVA KAKR┼áNEKOLI VRSTE, IZRECNEGA ALI POSREDNEGA, KAR VKLJU─îUJE, VENDAR NI OMEJENO NA POSREDNA JAMSTVA TR┼ŻNOSTI IN PRIMERNOSTI ZA DOLO─îEN NAMEN.

Lastnik avtorskih pravic za vse gradivo je IBM Corporation.

S presnetjem publikacije s te spletne strani ali njenim natisom se strinjate s temi dolo─Źbami in pogoji.

Natisnjeno na Danskem