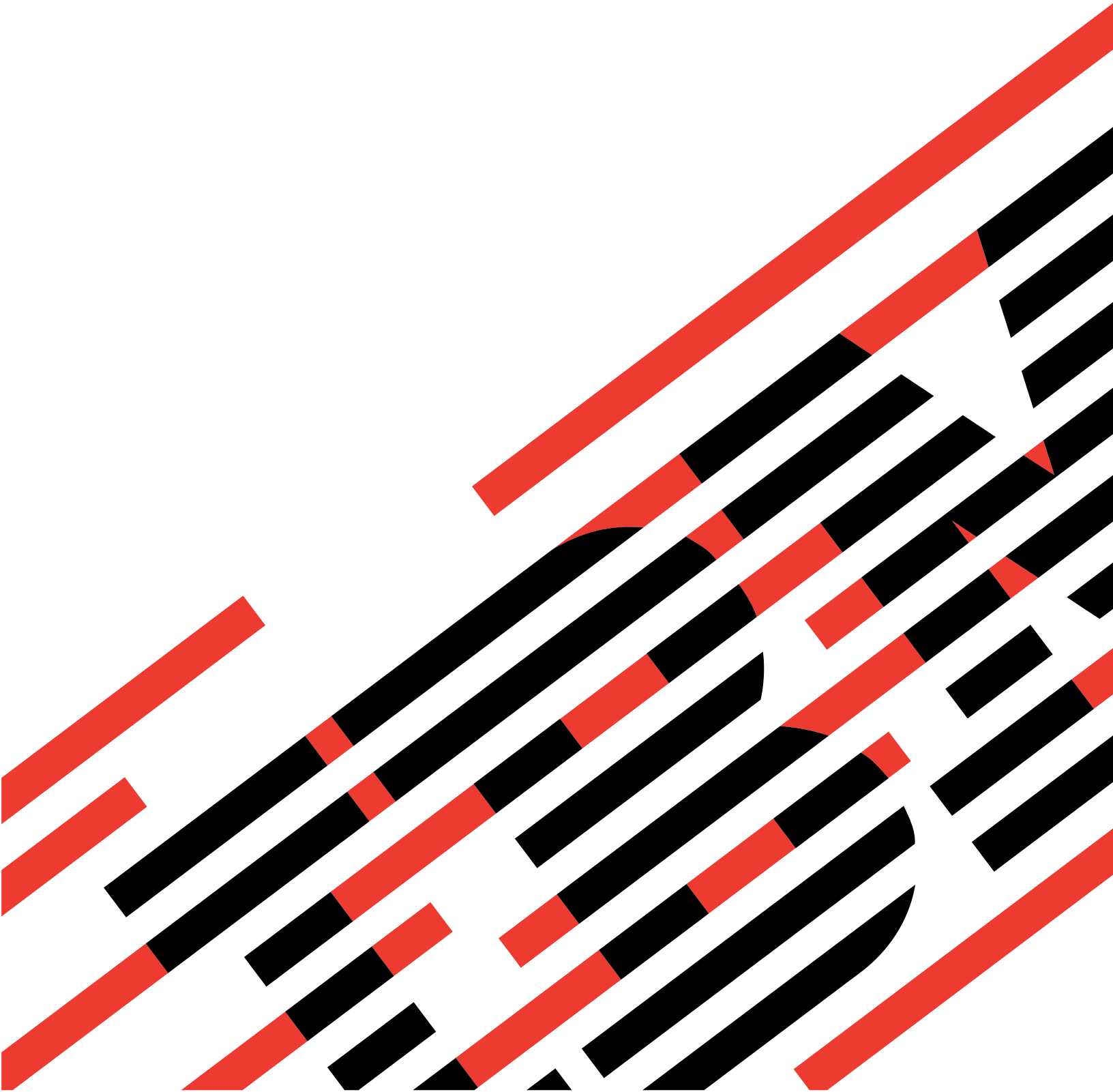
IBM

eserver

iSeries

Reţea privată virtuală

Versiunea 5 Ediţia 3



IBM

@server

iSeries

Reţea privată virtuală

Versiunea 5 Ediţia 3

Notă

Înainte de a utiliza aceste informaţii şi produsul pe care îl suportă, citiţi informaţiile din “Observaţii”, la pagina 67.

Ediţia a şasea (august 2005)

Această ediţie este valabilă pentru sistemul de operare IBM i5/OS (5722-SS1) Versiunea 5, Ediţia 3, Modificarea 2 şi pentru toate ediţiile şi modificările următoare, până când se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC (reduced instruction set computer), nici pe modelele CISC.

Cuprins

Lucrul în reţea privată virtuală

O reţea privată virtuală (VPN - virtual private network) permite companiei dumneavoastră să îşi extindă în siguranţă intranetul propriu în cadrul unei reţele publice, cum este Internet. Cu VPN, compania dumneavoastră poate controla traficul de reţea şi furniza caracteristici importante de securitate, cum ar fi autentificarea şi confidenţialitatea datelor.

VPN OS/400(R) este o componentă care se instalează opţional în Navigator iSeries(TM), interfaţa grafică cu utilizatorul (GUI) pentru OS/400. Ea vă permite să creaţi o cale sigură capăt-la-capăt pentru orice combinaţie de gazdă şi gateway. OS/400 VPN foloseşte metode de autentificare, algoritmi de criptare şi alte măsuri de precauţie pentru ca datele trimise între cele două puncte ale coenxiunii să rămână sigure.

VPN rulează la nivelul de reţea ale stivei de protocoale TCP/IP. Mai precis, VPN foloseşte cadrul de lucru deschis IPSec (IP Security Architecture). IPSec furnizează funcţii primare de securitate pentru Internet, precum şi elemente flexibile cu care puteţi crea reţele private virtuale robuste şi sigure.

VPN suportă deasemenea soluţii de tip L2TP (Layer 2 Tunnel Protocol). Conexiunile L2TP, numite şi linii virtuale, asigură un acces ieftin utilizatorilor de la distanţă, permiţând unui server din reţeaua companiei să gestioneze adresele IP atribuite utilizatorilor săi de la distanţă. În plus, conexiunile L2TP furnizează acces sigur la sistemul sau reţeaua dumneavoastră, când sunt protejate cu IPSec.

Este important să înţelegeţi efectul pe care îl va avea VPN asupra întregii dumneavoastră reţele. Planificarea şi implementarea corectă sunt esenţiale pentru succesul dumneavoastră. Revedeţi aceste subiecte pentru a vă asigura că ştiţi cum funcţionează VPN-urile şi cum aţi putea să le folosiţi:

Ce este nou pentru V5R3
Acest subiect prezintă informaţiile noi sau modificate semnificativ în această ediţie.

Tipăriţi acest subiect
Dacă preferaţi o versiune tipărită a acestor informaţii, de aici puteţi tipări PDF-ul.

Scenarii VPN
Revedeţi aceste scenarii pentru a vă familiariza cu tipurile VPN de bază şi cu paşii necesari pentru configurarea lor.

Conceptele VPN
Este important să aveţi cel puţin cunoştinţe de bază în ceea ce priveşte tehnologiile VPN standard. Acest subiect vă furnizează informaţii conceptuale despre protocoalele folosite de VPN.

Planificarea pentru VPN
Primul pas în utilizarea cu succes a VPN-ului este planificarea. Acest subiect furnizează informaţii despre migrarea de la ediţiile anterioare, cerinţele de setare şi legături către un consilier de planificare care va genera o foaie de lucru personalizată pentru specificaţiile dumneavoastră.

Configurarea VPN-ului
După planificarea pentru VPN, puteţi începe configurarea. Acest subiect vă oferă o prezentare generală a ceea ce puteţi face cu VPN şi în ce fel.

Gestionarea VPN-ului
Acest subiect descrie diferite operaţii cu care puteţi să vă gestionaţi conexiunile VPN active (de exemplu să le modificaţi, să le monitorizaţi sau să le ştergeţi).

Depanarea VPN-ului
Consultaţi acest subiect când aveţi probleme cu conexiunile VPN.

Informaţii înrudite despre VPN
Mergeţi aici pentru legături la alte surse de informaţii despre VPN şi subiecte înrudite.

Ce e nou pentru V5R3

Îmbunătăţirea funcţiei
Printre îmbunătăţirile funcţiei VPN (virtual private network - reţea privată virtuală) în Versiunea 5 Ediţia 3 (V5R3) se numără două noi tipuri de identificatori. La definirea politicilor de schimb chei VPN şi a punctelor finale de date ale conexiunii, pot fi selectate două noi tipuri de identificatori. Tipurile de identificatori includ adresa IP locală şi numele de gazdă IPv4. Pentru informaţii suplimentare, vedeţi ajutorul online din Navigator iSeries(TM).

- **Adresa mea IP locală**
  Tipul de identificator Adresa mea IP locală poate fi selectat pentru a specifica într-o definiţie de conexiune tipul de server de chei local pentru o politică Internet Key Exchange sau punctul final de date local. Când este selectat acesta, VPN-ul utilizează o adresă IPv4 disponibilă. Conexiunile VPN care utilizează acest tip identificator nu trebuie să folosească un filtru politică. În plus, sistemul local trebuie să fie iniţiatorul conexiunii.
- **Nume de gazdă IPv4**
  Identificatorul Nume de gadză IPv4 poate fi selectat pentru a defini câţiva parametri diferiţi:
  – Tipul de identificator pentru serverul de chei la distanţă într-o politică Internet Key Exchange
  – Identificatorul de adresă la distanţă din proprietăţile conexiunii
  – Definiţia filtrului politică pentru proprietăţile unui grup de conexiuni

  Numele de gazdă IPv4 rezolvă adresa IP a numelui de gazdă specificată ca tip de identificator.

Observaţie privind securitatea VPN:
Se recomandă să utilizaţi negocierea în modul principal de fiecare dată când este utilizată o cheie prepartajată pentru autentificare. În acest fel, schimbul este mai sigur. Dacă trebuie să utilizaţi chei prepartajate şi negocierea în modul agresiv, selectaţi cuvinte necunoscute, pentru care este mică probabilitatea de a fi sparte în atacurile care scanează un dicţionar de parole posibile. Pentru instrucţiuni despre cum să forţaţi un schimb de chei astfel încât să folosească negocierea în modul principal, vedeţi Riscuri privind securitatea la autentificarea cu chei prepartajate. Când creaţi sau editaţi o politică de schimb chei în Internet, puteţi de asemenea utiliza ajutorul online din Navigator iSeries pentru informaţii detaliate.

Îmbunătăţirea conţinutului
Printre modificările aduse subiectului V5R3 VPN din Centrul de informare se numără o prezentare virtuală care explică conceptul de tunel voluntar L2TP (Layer 2 Tunnel Protocol). Utilizaţi următoarele legături pentru a vedea o prezentare vizuală despre tuneluri voluntare L2TP protejate de IPSec. Aceasta necesită plug-in-ul Flash

. Alternativ, puteţi folosi versiunea HTML a acestei prezentări.

Cum să vedeţi ce e nou sau modificat

Pentru a vă ajuta să vedeţi ce modificări tehnice au fost făcute, aceste informaţii folosesc:

- Imaginea

  pentru a marca unde încep informaţii noi sau modificate.
- Imaginea

  pentru a marca unde se termină informaţiile noi sau modificate.

Pentru a afla alte informaţii despre ce este nou sau modificat la această ediţie, vedeţi Memo către utilizatori.

Tipăriţi acest subiect

Pentru a vedea sau descărca versiunea PDF a acestui document, selectaţi VPN (reţea privată virtuală) (în jur de 509 KB).

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia dumneavoastră de lucru pentru citire sau tipărire:

1. Faceţi clic dreapta pe PDF în browser (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Save Target As..**, dacă utilizaţi Internet Explorer. Faceţi clic pe **Save Link As...**, dacă utilizaţi Netscape Communicator.
3. Deplasaţi-vă la directorul în care vreţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

Aveţi nevoie de Acrobat Reader pentru a vedea sau tipări aceste PDF-uri. Puteţi descărca o copie de la situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)

.

Scenarii VPN

Revedeţi următoarele scenarii pentru a vă familiariza cu detaliile tehnice şi de configurare pe care le implică aceste tipuri de conexiune de bază:

- **Scenariu VPN: Conexiune de bază cu biroul filialei**
  În acest scenariu, compania dumneavoastră vrea să stabilească un VPN între subreţelele a două departamente la distanţă, printr-o pereche de calculatoare iSeries(TM) acţionând ca gateway-uri VPN.
- **Scenariu VPN: Conexiune de bază companie la companie**
  În acest scenariu, compania dumneavoastră vrea să stabilească un VPN între o staţie de lucru client din divizia dumneavoastră de producţie şi o staţie de lucru client din departamentul de aprovizionare al unui partener de afaceri.
- **Scenariu VPN: Protejarea unui tunel voluntar L2TP cu IPSec**
  Acest scenariu prezintă o conexiune între gazda dintr-un birou de filială şi un birou la companiei care foloseşte L2TP protejat de IPSec. Biroul filialei are o adresă IP alocată dinamic, în timp ce biroul companiei are o adresă IP statică, rutabilă global.
- **Scenariu VPN: Folosirea translatării adresei de reţea pentru VPN**
  În acest scenariu, compania dumneavoastră vrea să schimbe date confidenţiale cu unul dintre partenerii ei de afaceri utilizând VPN OS/400(R). Pentru a proteja şi mai mult structura reţelei, compania dumneavoastră va folosi de asemenea VPN NAT, pentru a ascunde adresa IP privată a serverului iSeries pe care îl foloseşte pentru a găzdui aplicaţiile la care are acces partenerul de afaceri.

Alte scenarii VPN

Pentru a vedea şi alte scenarii de configurare a VPN-ului, folosiţi aceste surse de informaţii despre VPN:

- **Scenariu QoS: Rezultate sigure şi predictibile (VPN şi QoS)**
  Puteţi crea politici de calitate a serviciului (QoS) cu VPN. Acest exemplu arată cum puteţi folosi VPN-ul şi QoS împreună.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153**

Acest manual IBM oferă un proces pas cu pas pentru configurarea tunelului VPN folosind VPN din V5R1 şi suportul L2TP şi IPSec integrat în Windows 2000.

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

  Acest manual explorează conceptele VPN şi descrie implementarea folosind securitate IP (IPSec) şi Layer 2 Tunneling Protocol (L2TP) pe OS/400.

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

  Acest manual explorează toate caracteristicile integrate de securitate a reţelei disponibile în sistemul OS/400, cum ar fi filtrele IP, NAT, VPN, server proxy HTTP, SSL, DNS, retransmiterea poştei, auditarea şi înregistrarea în istoric. Descrie utilizarea lor prin exemple practice.

Scenariu VPN: Conexiunea de bază cu biroul filialei

Să considerăm cazul în care compania dumneavoastră doreşte minimizarea costurilor rezultate din comunicarea cu şi între propriile filiale. În prezent, compania dumneavoastră foloseşte frame relay sau linii închiriate, dar vreţi să luaţi exploraţi şi alte opţiuni de transmitere a datelor confidenţiale interne, care sunt mai puţin costisitoare, mai seigure şi accesibile global. Prin exploatarea Internetului, puteţi realiza uşor o reţea privată virtuală (VPN) pentru a îndeplini necesităţile companiei dumneavoastră.

Compania dumneavoastră şi biroul său de filială au nevoie de protecţia unui VPN pe Internet, dar nu şi în interiorul propriilor intranet-uri. Considerând că intranet-urile sunt sigure, cea mai bună soluţie este să creaţi un VPN gateway-la-gateway. În acest caz, amândouă gateway-urile sunt conectate direct la reţeaua intermediară. Cu alte cuvinte, sunt sisteme *de graniţă* sau *periferice*, care nu sunt protejate de firewall-uri. Acest exemplu este util pentru a prezenta paşii de setare a unei configuraţii VPN de bază. Când acest scenariu se referă la termenul *Internet*, se referă la reţeaua care intermediară dintre cele două gateway-uri VPN, care ar putea fi reţeaua privată a companiei sau Internetul public.

> **Notă importantă:**
> În acest scenariu gateway-urile de securitate iSeries(TM) sunt legate direct la Internet. Absenţa unui firewall are intenţia de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile de securitate implicate de fiecare dată când vă conectaţi la Internet. Consultaţi AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> , pentru descrierea detaliată a diverselor metode de reducere a acestor riscuri.

Avantaje

Acest scenariu are următoarele avantaje:

- Folosirea Internetului sau a unui intranet existent reduce costul liniilor private între subreţele la distanţă.
- Folosirea Internetului sau a unui intranet existent reduce complexitatea instalării şi întreţinerii liniilor private şi a echipamentului asociat.
- Folosirea Internetului permite locaţiilor la distanţă să se conecteze aproape oriunde în lume.
- Folosirea VPN-ului furnizează utilizatorilor acces la toate serverele şi resursele de pe fiecare parte a conexiunii, ca şi când ar fi conectaţi folosind o linie închiriată sau o conexiune de tip reţea de arie întinsă (WAN).
- Folosirea metodelor standard de autentificare şi de criptare asigură securitatea informaţiilor sensibile, trimise de la o locaţie la alta.
- Schimbându-vă cheile de criptare dinamic şi în mod regulat, se simplifică instalarea şi se minimizează riscul decodificării cheilor şi străpungerea securităţii.

- Utilizarea adreselor IP în fiecare subreţea la distanţă face nenecesară alocarea adreselor IP publice pentru fiecare client.

Obiective

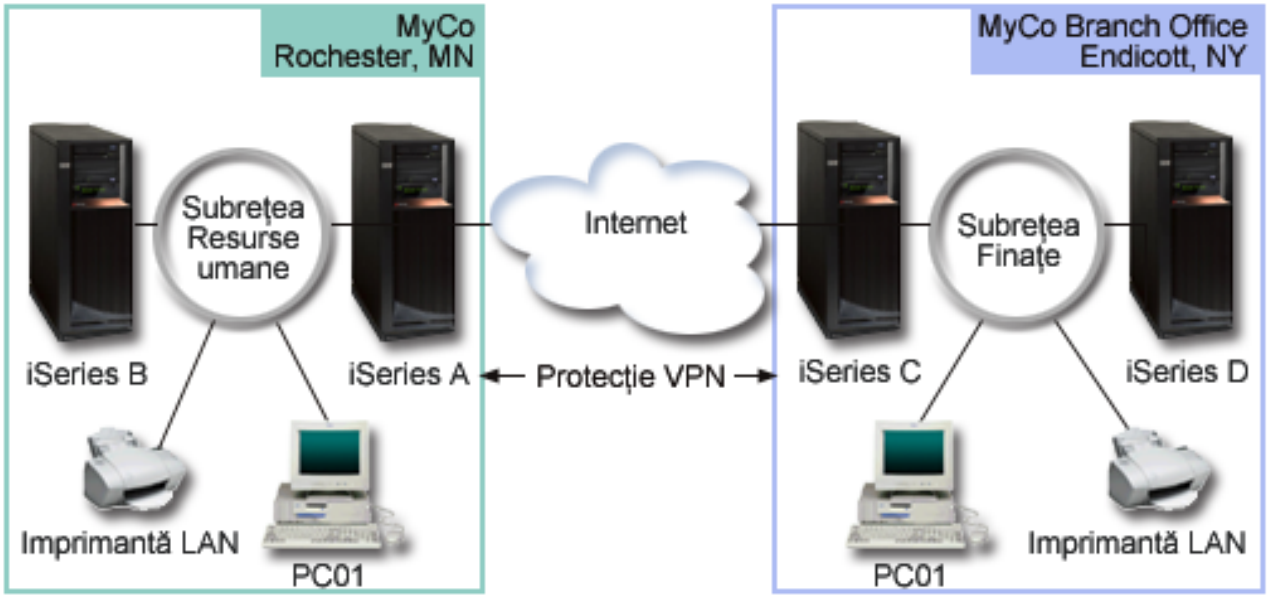
În acest scenariu, MyCo, Inc. vrea să stabilească un VPN între subreţelele departamentelor proprii de Resurse Umane şi Finanţe, printr-o pereche de servere iSeries. Cele două servere se vor comporta ca gateway-uri VPN. Într-o configuraţie VPN, un gateway gestionează cheile şi aplică IPSec datelor care se transmit prin tunel. Gateway-urile nu sunt punctele finale de date ale conexiunii.

Obiectivele acestui scenariu sunt următoarele:

- VPN trebuie să protejeze tot traficul de date între subreţeaua departamentului Resurse Umane şi cea a departamentului Finanţe.
- Traficul de date nu necesită protecţia VPN-ului după ce ajunge la una dintre subreţelele departamentelor.
- Toţi clienţii şi gazdele din fiecare reţea au acces total la reţeaua celuilalt, inclusiv toate aplicaţiile.
- Serverele gateway pot comunica între ele şi îşi pot accesa aplicaţiile între ele.

Detalii

Următoarea ilustraţie prezintă caracteristicile reţelei MyCo.



Departamentul Resurse Umane

- Pe iSeries-A rulează OS/400(R) versiunea 5 ediţia 2 (V5R2) şi el se comportă ca un gateway VPN al Departamentului Resurse Umane.
- Subreţeaua este 10.6.0.0 cu masca 255.255.0.0. Această subreţea reprezintă punctul final de date al tunelului VPN, la sediul MyCo Rochester.
- iSeries-A se conectează la Internet cu adresa IP 204.146.18.227. Acesta este punctul final al conexiunii. Cu alte cuvinte, iSeries-A realizează gestionarea cheilor şi aplică IPSec datagramelor IP care vin şi pleacă.
- iSeries-A se conectează la propriile subreţele cu adresa IP 10.6.11.1.
- iSeries-B este un server de producţie din subreţeaua Resurse Umane, care rulează aplicaţii TCP/IP standard.

Departamentul Finanţe

- Pe iSeries-C rulează OS/400 versiunea 5 ediţia 2 (V5R2) şi el se comportă ca gateway VPN al departamentului Finanţe.
- Subreţeaua este 10.196.8.0 cu masca 255.255.255.0. Această subreţea reprezintă punctul final de date al tunelului VPN, la sediul MyCo Endicott.
- iSeries-C se conectează la Internet cu adresa IP 208.222.150.250. Acesta este punctul final al conexiunii. Cu alte cuvinte, iSeries-C realizează gestionarea cheilor şi aplică IPSec datagramelor IP care vin şi pleacă.
- iSeries-C se conectează la propriile subreţele cu adresa IP 10.196.8.5.

Operaţiile de configurare

Trebuie să executaţi fiecare dintre aceste operaţii pentru a configura conexiunea la biroul filialei, descrisă în acest scenariu:

1. Verificaţi rutarea TCP/IP, pentru a vedea dacă cele două servere gateway pot comunica între ele prin Internet. În acest fel, vă asiguraţi că gazdele din fiecare subreţea rutează corespunzător la gateway-ul corespondent pentru accesul la subreţeaua la distanţă.
   Notă: Rutatea nu este unul dintre obiectivele vizate de acest subiect. Dacă aveţi întrebări, vedeţi Rutarea TCP/IP şi echilibrarea sarcinii de lucru, în Centrul de informare.
2. Parcurgeţi (pagină 6) foile de lucru pentru planificare şi listele de verificare pentru ambele sisteme.
3. Configuraţi (pagină 7) VPN-ul pe gateway-ul VPN de la Resurse Umane (iSeries-A).
4. Configuraţi (pagină 8) VPN-ul pe gateway-ul VPN de la Finanţe (iSeries-C).
5. Asiguraţi-vă ca serverele VPN sunt ponite (pagină 8)
6. Testaţi (pagină 8) comunicaţiile dintre cele două subreţele la distanţă.

Detalii de configurare

După ce aţi făcut primul pas, verificând că rutarea TCP/IP funcţionează corespunzător şi că serverele dumneavoastră gateway pot comunica, sunteţi gata să începeţi configurarea VPN.

Pasul 2: Completaţi foile de lucru pentru planificare

Următoarele liste de verificări pentru planificare arată tipul de informaţii de care aveţi nevoie înainte de a începe configurarea VPN. Toate răspunsurile din lista de verificare a cerinţei preliminare trebuie să fie Da înainte de a continua cu setarea VPN.

Notă: Aceste foi de lucru sunt valabile pentru iSeries-A. Se repetă procesul pentru iSeries-C, înlocuind adresele IP după cum este necesar.

Cerinţe preliminare	**Răspunsuri**
Sistemul dumneavoastră de operare este OS/400(R) V5R2 (5722-SS1) sau ulterior?	Da
Este instalată opţiunea Digital Certificate Manager (5722-SS1 Option 34)?	Da
Este instalat Cryptographic Access Provider (5722-AC2 sau AC3)?	Da
Este instalat iSeries(TM) Access for Windows(R) (5722-XE1)?	Da
Este instalat Navigator iSeries?	Da
Este instalată subcomponenta Reţea a Navigatorului iSeries?	Da
Este instalat TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Da
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe iSeries (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da

Cerinţe preliminare	Răspunsuri
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH şi ESP?	Da
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	Da

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul	Răspunsuri
Ce tip de conexiune creaţi?	gateway-la-gateway
Cum veţi denumi grupul de chei dinamice?	HRgw2FINgw
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile?	echilibrate
Folosiţi certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată?	Nu topsecretstuff
Care este identificatorul serverului de chei local?	Adresa IP: 204.146.18.227
Care este identificatorul punctului final de date local?	Subreţea: 10.6.0.0 Mască: 255.255.0.0
Care este identificatorul serverului de chei la distanţă?	Adresa IP: 208.222.150.250
Care este identificatorul punctului final de date la distanţă?	Subreţea: 10.196.8.0 Mască: 255.255.255.0
Ce porturi şi protocoale doriţi să permiteţi să treacă prin conexiune?	Oricare
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja datele?	echilibrate
La care interfeţe se aplică conexiunea?	TRLINE

Pasul 3: Configuraţi VPN-ul pe iSeries-A

Folosiţi informaţiile din foile dumneavoastră de lucru pentru a configura VPN-ul pe iSeries-A, după cum urmează:

1. În Navigator iSeries, expandaţi iSeries-A **—>Reţea —>Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune nouă.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi HRgw2FINgw.
6. (opţional) Specificaţi o descriere pentru acest grup de conexiune.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gateway-ului dumneavoastră la alt gateway**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.
11. Apăsaţi pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectaţi **Nu** pentru a indica faptul că nu veţi folosi certificate pentru autentificarea conexiunii.
13. Apăsaţi **Următor** pentru a merge la pagina **Server de chei local**.
14. Selectaţi **Adresă IP Versiunea 4** din câmpul **Tip identificator**.
15. Selectaţi 204.146.18.227 din câmpul **Adresă IP**.
16. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
17. Selectaţi **Adresă IP Versiunea 4** în câmpul **Tip identificator**.
18. Introduceţi 208.222.150.250 în câmpul **Identificator**.
19. Introduceţi topsecretstuff în câmpul **Cheie prepartajată**.

20. Apăsaţi **Următor** pentru a merge la pagina **Punct final local de date**.
21. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
22. Introduceţi 10.6.0.0 în câmpul **Identificator**.
23. Introduceţi 255.255.0.0 în câmpul **Mască subreţea**.
24. Apăsaţi **Următor** pentru a merge la pagina **Punct final de date distanţă**.
25. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
26. Introduceţi 10.196.8.0 în câmpul **Identificator**.
27. Introduceţi 255.255.255.0 în câmpul **Mască subreţea**.
28. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
29. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge la pagina **Politică de date**.
30. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**. Selectaţi **Folosire algoritm de criptare RC4**.
31. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
32. Selectaţi **TRLINE** din tabelul **Linie**.
33. Apăsaţi **Următor** pentru a merge la pagina **Sumar**. Treceţi în revistă obiectele pe care le va crea vrăjitorul, pentru a vă asigura că sunt corecte.
34. Apăsaţi **Sfârşit** pentru a încheia configurarea.
35. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Da, activare filtre de politică generarate**, apoi selectaţi **Permitere totală a celuilalt trafic**. Apăsaţi **OK** pentru a încheia configurarea. Când veţi fi întrebat, specificaţi că doriţi să activaţi regulile pe alte interfeţe.

Aţi terminat de configurat VPN pe iSeries-A. Următorul pas este să configuraţi VPN pe gateway-ul VPN al departamentului Finanţe (iSeries-C).

Pasul 4: Configuraţi VPN-ul pe iSeries-C

Parcurgeţi aceiaşi paşi ca la configurarea iSeries-A, înlocuind adresele IP după cum e necesar. Folosiţi ca ghid foile de lucru pentru planificare. După ce terminaţi de configurat gateway-ul VPN al departamentului Finanţe, conexiunile dumneavoastră vor fi într-o stare *la-cerere*, ceea ce înseamnă că pornesc atunci când sunt trimise datagramele IP pe care trebuie să le protejeze această conexiune VPN. Următorul pas este să porniţi serverele VPN, dacă nu sunt deja pornite.

Pasul 6: Porniţi serverele VPN

Parcurgeţi paşii următori pentru a porni serverele VPN:

1. În Navigator iSeries, expandaţi **serverul —>Reţea —>Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Pornire**.

Pasul 7: Testaţi conexiunea

După ce aţi terminat de configurat ambele servere şi aţi pornit cu succes serverele VPN, testaţi conectivitatea pentru a vă asigura că subreţelele la distanţă pot comunica una cu cealaltă. Pentru aceasta, parcurgeţi paşii următori:

1. În Navigator iSeries, expandaţi **iSeries-A —>Reţea**.
2. Faceţi clic dreapta pe **Configurare TCP/IP** şi selectaţi **Utilitare** şi apoi selectaţi **Ping**.
3. În caseta de dialog **Ping de la**, introduceţi iSeries-C în câmpul **Ping**.
4. Faceţi clic pe **Ping acum** pentru verificarea conectivităţii de la iSeries-A la iSeries-C.
5. Faceţi clic pe **OK** când aţi terminat.

Scenariu VPN: Conexiune de bază companie la companie

Multe companii folosesc frame relay sau linii închiriate pentru comunicaţii sigure cu partenerii lor de afaceri, finanţatori şi furnizori. Din păcate, aceste soluţii sunt mai întotdeauna scumpe şi limitate geografic. VPN oferă o soluţie alternativă pentru companiile care vor comunicaţii private cu cost redus.

Se consideră situaţia în care sunteţi un furnizor important de subansamble al unui producător. Pentru că este vital să aveţi produsele specifice şi cantităţile exact la timpul cerut de firma producătoare, trebuie să dispuneţi mereu de starea inventarului producătorului şi de programele de producţie. Poate că în prezent realizaţi această interacţiune manual şi constataţi că este mare consumatoare de timp, implică un cost ridicat şi uneori apar date eronate. Ca urmare, vreţi să găsiţi o cale mai uşoară, mai rapidă şi mai eficientă pentru comunicarea cu compania producătorului. Având în vedere confidenţialitatea cestor informaţii, producătorul nu doreşte să le publice pe propriul sit Web sau să le distribuie lunar printr-un raport extern. Exploatând Internetul public, puteţi stabili uşor o reţea privată virtuală (VPN), pentru a satisface nevoile ambelor companii.

Obiective

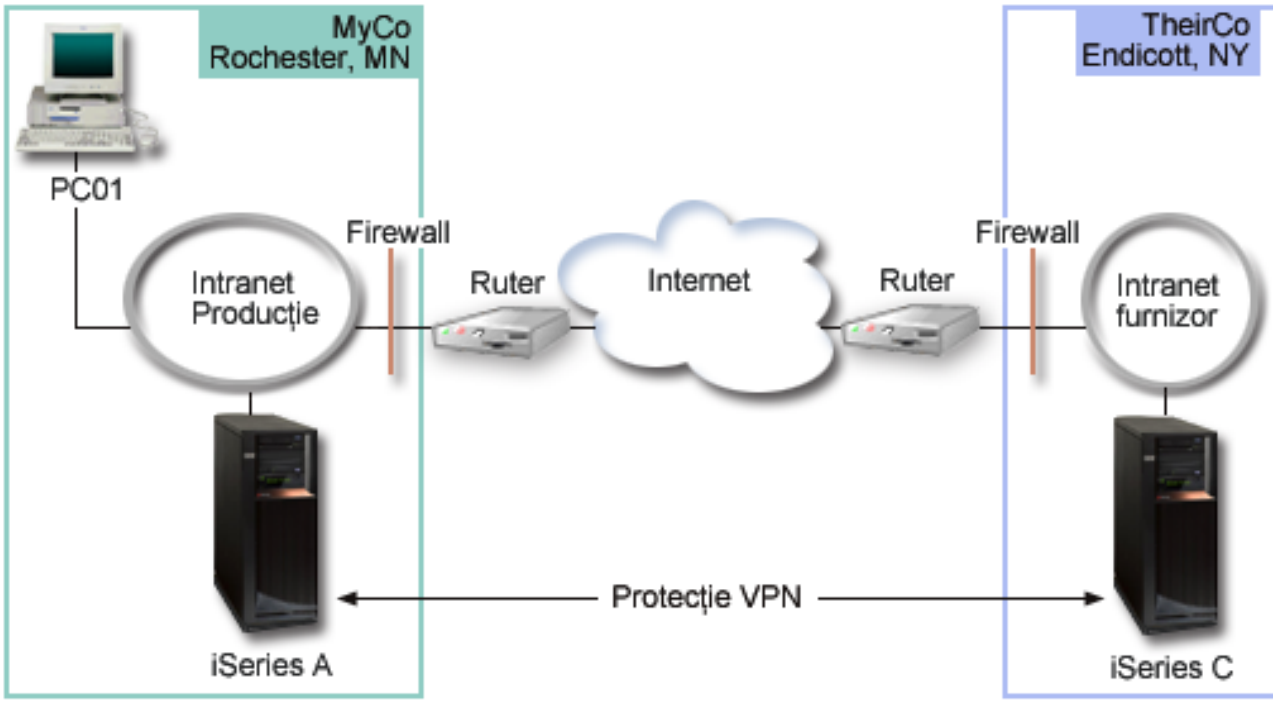
În acest scenariu, MyCo vrea să stabilească un VPN între o gazdă din divizia sa de subansamble şi o gazdă din departamentul de producţie al unuia dintre partenerii de afaceri, TheirCo.

Pentru că informaţiile partajate de aceste două companii sunt de înaltă confidenţialitate, trebuie să fie protejate atât timp cât traversează Internetul. În plus, datele nu trebuie să circule neprotejate în reţelele interne ale celor două comapanii, deoarece fiecare reţea o consideră pe cealaltă nesigură. Cu alte cuvinte, cele două companii au nevoie de autentificare end-to-end, integritate şi criptare.

Notă importantă
Intenţia acestui scenariu este să facă o prezentare introductivă, prin exemplu, a unei configuraţii VPN simple gazdă-la-gazdă. Într-un mediu de reţea tipic, va trebuie să luaţi în considerare şi configurarea unui firewall, cerinţele de adresare IP şi rutarea, printre altele.

Detalii

Următoarea ilustraţie prezintă caracteristicile de reţea ale MyCo şi TheirCo:



Reţeaua de aprovizionare MyCo

- Pe iSeries-A rulează OS/400(R) versiunea 5 ediţia 2 (V5R2).

- iSeries-A are o adresă IP 10.6.1.1. Aceasta este punctul final al conexiunii, precum şi punctul final de date. Aceasta pentru că iSeries-A realizează negocieri IKE şi aplică IPSec datagramelor IP de intrare şi ieşire şi este de asemenea sursa şi destinaţia pentru datele care circulă prin VPN.
- iSeries-A este în subreţeaua 10.6.0.0 cu masca 255.255.0.0
- Doar iSeries-A poate iniţia conexiunea cu iSeries-C.

Reţeaua de producţie a TheirCo

- Pe iSeries-C rulează OS/400 versiunea 5 ediţia 2 (V5R2).
- iSeries-C are o adresă IP 10.196.8.6. Aceasta este punctul final al conexiunii, precum şi punctul final de date. Aceasta pentru că iSeries-A realizează negocieri IKE şi aplică IPSec datagramelor IP de intrare şi ieşire şi este de asemenea sursa şi destinaţia pentru datele care circulă prin VPN.
- iSeries-C este în subreţeaua 10.196.8.0 cu masca 255.255.255.0

Operaţiile de configurare

Trebuie să executaţi fiecare dintre aceste operaţii pentru a configura conexiunea de tip companie la companie, descrisă în acest scenariu:

1. Verificaţi rutarea TCP/IP pentru a vă asigura că iSeries-A şi iSeries-C pot comunica unul cu celălalt prin Internet. În acest fel, vă asiguraţi că gazdele din fiecare subreţea rutează corespunzător către gateway-ul corespunzător pentru a accesa subreţeaua la distanţă. Ţineţi cont că pentru acest scenariu va trebui să aveţi în vedere rutarea unor adrese private pe care nu le-aţi avut mai înainte.

   Notă: Rutatea nu este unul dintre obiectivele vizate de acest subiect. Dacă aveţi întrebări, vedeţi subiectul Rutarea TCP/IP şi echilibrarea sarcinii de lucru, în Centrul de informare.
2. Parcurgeţi (pagină 10) foile de lucru pentru planificare şi listele de verificare pentru ambele sisteme.
3. Configuraţi (pagină 11) VPN-ul pe iSeries-A, în reţeaua de aprovizionare a MyCo's.
4. Configuraţi (pagină 12) VPN-ul pe iSeries-C, în reţeaua de producţie a TheirCo's.
5. Activaţi (pagină 12) regulile de filtrare pe amândouă serverele.
6. Porniţi (pagină 13) conexiunea de pe iSeries-A.
7. Testaţi (pagină 13) comunicaţiile dintre cele două subreţele la distanţă.

Detalii de configurare

După ce finalizaţi primul pas, în care aţi verificat că rutarea TCP/IP funcţionează corespunzător şi serverele dumneavoastră pot comunica, sunteţi gata pentru a configura VPN-ul.

Pasul 2: Completaţi foile de lucru pentru planificare

Următoarele liste de verificări pentru planificare arată tipul de informaţii de care aveţi nevoie înainte de a începe configurarea VPN. Toate răspunsurile din lista de verificare a cerinţei preliminare trebuie să fie Da înainte de a continua cu setarea VPN.

Notă: Aceste foi de lucru sunt valabile pentru iSeries-A. Se repetă procesul pentru iSeries-C, înlocuind adresele IP după cum este necesar.

Cerinţe preliminare	Răspunsuri
Sistemul dumneavoastră de operare este OS/400(R) V5R2 (5722-SS1) sau ulterior?	Da
Este instalată opţiunea Digital Certificate Manager (5722-SS1 Option 34)?	Da
Este instalat Cryptographic Access Provider (5722-AC2 sau AC3)?	Da
Este instalat iSeries(TM) Access for Windows(R) (5722-XE1)?	Da
Este instalat Navigator iSeries ?	Da
Este instalată subcomponenta Reţea a Navigatorului iSeries?	Da
Este instalat TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Da

Cerinţe preliminare	Răspunsuri
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe iSeries (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH şi ESP?	Da
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	Da

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul	Răspunsuri
Ce tip de conexiune creaţi ?	gazdă-la-gazdă
Cum veţi denumi grupul de chei dinamice?	MyCo2TheirCo
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile?	cele mai înalte
Folosiţi certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată?	Da
Care este identificatorul serverului de chei local?	Adresa IP: 10.6.1.1
Care este identificatorul punctului final de date local ?	Adresa IP: 10.6.1.1
Care este identificatorul serverului de chei la distanţă ?	Adresa IP: 10.196.8.6
Care este identificatorul punctului final de date la distanţă ?	Adresa IP: 10.196.8.6
Ce porturi şi protocoale doriţi să permiteţi prin conexiune ?	Oricare
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja datele?	cele mai înalte
Pe care dintre interfeţe se aplică această conexiune ?	TRLINE

Pasul 3: Configuraţi VPN-ul pe iSeries-A

Folosiţi informaţiile din foile dumneavoastră de lucru pentru a configura VPN-ul pe iSeries-A, după cum urmează:

1. În Navigator iSeries, expandaţi-vă serverul **—>Reţea —>Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi MyCo2TheirCo.
6. (opţional) Specificaţi o descriere pentru acest grup de conexiuni.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gazdei dumneavoastră la altă gazdă**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Crearea unei noi politici** şi apoi selectaţi **Cea mai înaltă securitate, ce mai joasă performanţă**.
11. Apăsaţi pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectaţi **Da** pentru a indica dacă veţi folosi certificate pentru autentificarea conexiunii. Apoi, selectaţi certificatele care reprezintă iSeries-A.
    Notă: Dacă vreţi să folosiţi un certificat pentru autentificarea punctului final al conexiunii locale, trebuie să creaţi întâi certificatul în managerul de certificate digital (DCM).
13. Apăsaţi **Următor** pentru a merge în pagina **Identificator de punct final al conexiunii locale** .

14. Selectaţi **Adresa IP Versiunea 4** ca tip de identificator. Adresa IP asociată trebuie să fie 10.6.1.1. Din nou, aceste informaţii sunt definite în certificatul pe care îl creaţi în DCM.
15. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
16. Selectaţi **Adresa IP Versiunea 4** din câmpul **Tip de identificator**.
17. Introduceţi 10.196.8.6 în câmpul **Identificator**.
18. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
19. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge în pagina **Politică de date**.
20. Selectaţi **Crearea unei noi politici** şi apoi selectaţi **Cea mai înaltă securitate, cea mai joasă performanţă**. Selectaţi **Folosirea algoritmului de criptare RC4**.
21. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
22. Selectaţi **TRLINE**.
23. Apăsaţi **Următor** pentru a merge la pagina **Sumar**. Revedeţi obiectele pe care le va crea pentru a asigura corectitudinea lor.
24. Apăsaţi pe **Sfârşit** pentru a completa configurarea.
25. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Nu, regulile pachet vor fi activate la un moment ulterior** apoi faceţi clic pe **Ok**.

Următorul pas este să se specifice faptul că doar iSeries-A poate iniţia această conexiune. Realizaţi aceasta prin personalizarea proprietăţilor grupului de chei dinamice, MyCo2TheirCo, pe care l-a creat vrăjitorul:

1. Faceţi clic pe **După grup** în panoul din stânga al interfeţei VPN şi grupul nou de chei dinamice, MyCo2TheirCo, va fi afişat în panoul din dreapta. Faceţi clic dreapta pe el şi selectaţi **Proprietăţi**.
2. Mergeţi la pagina **Polică** şi selectaţi opţiunea **Sistemul local iniţiază conexiunea**.
3. Apăsaţi **OK** pentru a salva modificările.

Aţi terminat de configurat VPN pe iSeries-A. Următorul pas este de a configura VPN pe iSeries-C în reţeaua de producţie TheirCo.

Pasul 4: Configuraţi VPN-ul pe iSeries-C

Parcurgeţi aceiaşi paşi ca la configurarea iSeries-A, înlocuind adresele IP după cum e necesar. Folosiţi ca ghid foile de lucru pentru planificare. Când terminaţi configurarea iSeries-C, trebuie să activaţi regulile de filtrare pe care vrăjitorul Conexiune le-a creat pe fiecare server.

Pasul 5: Activaţi regulile de pachete

Vrăjitorul creează automat regulile de pachete pe care această conexiune le cere pentru a funcţiona corespunzător. Oricum, trebuie să le activaţi pe ambele sisteme înainte de a porni conexiunea VPN. Pentru a face acest lucru pe iSeries-A, parcurgeţi paşii următori:

1. În Navigator iSeries, expandaţi **iSeries-A —>Reţea —>Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachete** şi selectaţi **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectaţi dacă vreţi să activaţi doar regulile generate VPN, doar un fişier selectat sau ambele variante. Puteţi alege ultima variantă, de exemplu, dacă aveţi diverse reguli PERMITERE şi REFUZARE pe care doriţi să le impuneţi pe interfaţă în plus faţă de regulile generate VPN.
4. Selectaţi interfaţa pe care vreţi să activaţi regulile. În acest caz, selectaţi **Toate interfeţele**.
5. Faceţi clic pe **OK** în caseta de dialog pentru a confirma ca vreţi să verificaţi şi să activaţi regulile pe interfaţa sau interfeţele specificate. După ce aţi apăsat OK, sistemul verifică regulile de erori sintactice şi semantice şi raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fişier anume şi un număr de linie, puteţi apăsa clic dreapta pe eroare şi selecta **Mergi la linie** pentru a evidenţia eroarea în fişier.
6. Repetaţi aceşti paşi pentru a activa regulile de pachete pe iSeries-C.

Pasul 6: Porniţi conexiunea

Parcurgeţi paşii următori pentru a porni conexiunea MyCo2TheirCo de la iSeries-A:

1. În Navigator iSeries, expandaţi **iSeries-A —>Reţea —>Politici IP**.
2. Dacă serverul VPN nu este pornit, faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Pornire**. Aceasta porneşte serverul VPN.
3. Expandaţi **Reţea privată virtuală —>Conexiuni sigure**.
4. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
5. Faceţi clic dreapta pe **MyCo2TheirCo** şi selectaţi **Pornire**.
6. Din meniul **Vizualizare**, selectaţi **Reîmprospătare**. Dacă conexiunea porneşte cu succes, starea se va modifica din *Inactivă* în *Activată*. Pot trece câteva minute până porneşte conexiunea, aşa că trebuie să reîmprospătaţi periodic până când starea se schimbă la *Activată*.

Pasul 7: Testaţi conexiunea

După ce aţi terminat de configurat ambele servere şi aţi pornit cu succes conexiunile, testaţi conectivitatea pentru a vă asigura că gazdele la distanţă pot comunica una cu cealaltă. Pentru aceasta, parcurgeţi paşii următori:

1. În Navigator iSeries, expandaţi **iSeries-A —>Reţea**.
2. Faceţi clic dreapta pe **Configurarea TCP/IP** şi selectaţi **Utilitare** şi apoi selectaţi **Ping**.
3. Din caseta de dialog **Ping de la**, introduceţi iSeries-C în câmpul **Ping**.
4. Faceţi clic pe **Ping acum** pentru verificarea conectivităţii de la iSeries-A la iSeries-C.
5. Faceţi clic pe **OK** când aţi terminat.

Scenariu VPN: Protejarea unui tunel voluntar L2TP cu IPSec

Să presupunem că compania dumneavoastră are un mic birou de filială în alt stat. În oricare zi de lucru biroul filialei ar putea cere acces la informaţii confidenţiale despre un iSeries(TM) din reţeaua internă a companiei dumneavoastră. Compania dumneavoastră foloseşte în prezent o linie închiriată scumpă pentru a furniza accesul biroului filială la reţeaua companiei. Deşi compania dumneavoastră doreşte să asigure în continuare un acces sigur la intranet, în ultimă în cele din urmă doriţi să reduceţi costul pe care îl implică linia închiriată. Aceasta se poate realiza prin crearea unui tunel voluntar Layer 2 Tunnel Protocol (L2TP) pentru a vă extinde reţeaua companiei, astfel ca biroul filialei să apară ca o parte a subreţelei companiei. VPN protejează traficul de date prin tunelul L2TP.

Cu un tunel voluntar L2TP, biroul filialei de la distanţă stabileşte un tunel direct la serverul de reţea L2TP (LNS) al reţelei companiei. Funcţionalitatea concentratorului de acces L2TP (LAC) se află la client. Tunelul este transparent pentru furnizorul de servicii Internet (ISP) al clientului de la distanţă, astfel că ISP-ul nu trebuie să suporte L2TP. Dacă vreţi să citiţi mai multe despre conceptele L2TP, vedeţi L2Tp (Layer 2 Tunnel Protocol).

> **Notă importantă:**
> În acest scenariu gateway-urile de securitate iSeries sunt ataşate direct la Internet. Absenţa unui firewall are intenţia de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile de securitate implicate de fiecare dată când vă conectaţi la Internet. Consultaţi AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00
>
> 
>
> , pentru descrierea detaliată a diverselor metode de reducere a acestor riscuri.

Obiective

În acest scenariu, un iSeries dintr-un birou de filială se conectează la reţeaua companiei printr-un gateway iSeries cu un tunel L2TP protejat cu VPN.

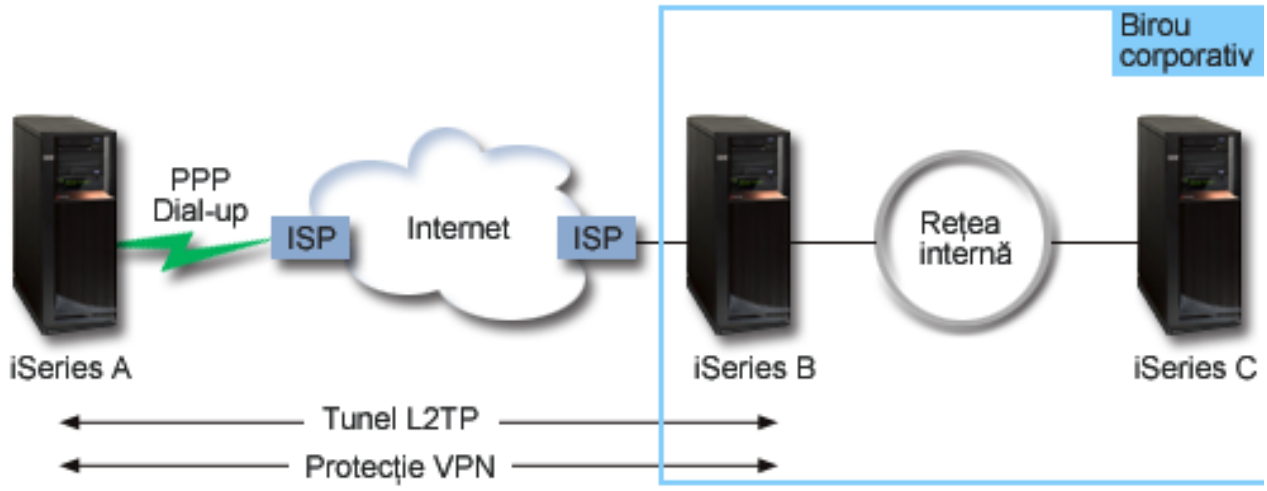
Obiectivele principale ale acestui scenariu sunt:

- Biroul de filială iniţiază întotdeauna conexiunea la biroul companiei.

- Sistemul biroului de filială este singurul sistem din reţeaua biroului de filială care are nevoie de acces la reţeaua companiei. Cu alte cuvinte, rolul său este acela al unei gazde, nu al unui gateway, în reţeaua biroului de filială.
- Sistemul companiei este un calculator gazdă din reţeaua biroului companiei.

Detalii

Următoarea ilustraţi prezintă caracteristicile reţelei pentru acest scenariu:



iSeries-A

- Trebuie să aveţi acces la aplicaţii TCP/IP pe toate sistemele din reţeua companiei.
- Primeşte adrese IP alocate dinamic de la ISP-ul său.
- Trebuie să fie configurat să furnizeze suport L2TP.

iSeries-B

- Trebuie să aibă acces la aplicaţii TCP/IP de pe iSeries-A.
- Subreţeaua este 10.6.0.0 cu masca 255.255.0.0. Această subreţea reprezintă punctul final de date al tunelului VPN la sediul companiei.
- Se conectează la Internet cu adresa IP 205.13.237.6. Acesta este punctul final al conexiunii. Adică, iSeries-B realizează gestionarea de chei şi aplică IPSec la datagamele IP care intră şi care ies. iSeries-B se conectează la subreţeaua sa cu adresa IP 10.6.11.1.

În termeni L2TP, *iSeries-A* funcţionează ca iniţiatorul L2TP, în timp ce *iSeries-B* funcţionează ca terminator L2TP.

Operaţiile de configurare

Presupunând că deja există şi funcţionează configurarea TCP/IP, trebuie să executaţi următoarele operaţii:

1. Configuraţi VPN-ul (pagină 15) pe iSeries-A.
2. Configuraţi (pagină 16) un profil de conexiune PPP şi linie virtuală pentru iSeries-A.
3. Aplicaţi (pagină 17)grupul de chei dinamice la profilul PPP.
4. Configuraţi VPN-ul (pagină 18) pe iSeries-B.
5. Configuraţi (pagină 18) un profil de conexiune PPP şi linie virtuală pentru iSeries-B.
6. Activaţi (pagină 19) regulile pachet pe iSeries-A şi iSeries-B.
7. Porniţi (pagină 19) conexiunile de la iSeries-A.

Detalii de configurare

După ce verificaţi că TCP/IP funcţionează corespunzător şi că serverele dumneavoastră iSeries(TM) pot comunica, sunteţi gata pentru a începe configurarea conexiunii descrise în acest scenariu.

Pasul 1: Configuraţi VPN-ul pe iSeries-A

Urmaţi aceşti paşi pentru a configura VPN-ul pe iSeries-A:

1. **Configurarea politicii Internet Key Exchange**
   a. În Navigator iSeries, expandaţi iSeries-A **—> Reţea—> Politici IP—> Reţea privată virtuală—> Politici de securitate IP** .
   b. Faceţi clic dreapta pe **Politici Internet Key Exchange** şi selectaţi **Politică nouă Internet Key Exchange**
   c. În pagina **Server la distanţă**, selectaţi **Adresă IP Versiunea 4** drept tipul de identificator şi apoi introduceţi 205.13.237.6 în câmpul **Adresa IP**.
   d. În pagina **Asocieri**, selectaţi **Cheie prepartajată** pentru a indica faptul că această conexiune foloseşte o cheie prepartajată pentru a autentifica această politică.
   e. Introduceţi cheia prepartajată în câmpul **Cheie**. Trataţi cheia prepartajată ca pe o parolă.
   f. Selectaţi **Identificator cheie** pentru tipul identificatorului serverului de chei local şi apoi introduceţi identificatorul cheii în câmpul **Identificator**. De exemplu, thisisthekeyid. Reţineţi că serverul de chei local are o adresă IP atribuită dinamic, care este imposibil de cunoscut înainte. iSeries-B foloseşte acest identificator pentru a identifica iSeries-A când iSeries-A iniţiază o conexiune.
   g. În pagina **Transformări**, apăsaţi **Adăugare** pentru a adăuga transformări pe care iSeries-A le propune lui iSeries-B pentru protecţia cheilor şi pentru a specifica dacă politica IKE foloseşte protecţia identităţii când iniţiază negocierile din faza 1.
   h. În pagina **Transformare politică IKE**, selectaţi **Cheie prepartajată** pentru metoda de autentificare, **SHA** pentru algoritmul hash şi **3DES-CBC** pentru algoritmul de criptare. Acceptaţi valorile implicite pentru grupul Diffie-Hellman şi pentru Expirare chei IKE după.
   i. Apăsaţi **OK** pentru a reveni la pagina **Transformări**.
   j. Selectaţi **Negociere în mod agresiv IKE (fără protecţie de identitate).**

   »

   Notă: Dacă folosiţi chei prepartajate şi negociere în modul agresiv în configuraţia dumneavoastră, selectaţi pentru parole cuvinte necunoscute, pentru care este mică probabilitatea de a fi sparte în atacurile care scanează un dicţionar. Se recomandă de asemenea să vă modificaţi periodic parolele

   «

   k. Apăsaţi **OK** pentru a salva configuraţia.
2. **Configurare politică de date**
   a. Din interfaţa VPN, faceţi clic dreapta pe **Politici de date** şi selectaţi **Politică nouă de date**.
   b. În pagina **General**, specificaţi numele politicii de date. De exemplu, l2tpremoteuser.
   c. Mergeţi la pagina **Propuneri**. O propunere este o colecţie de protocoale pe care le folosesc serverele de chei iniţiante şi respondente pentru a stabili o conexiune dinamică între două capete. Puteţi folosi o singură politică de date în mai multe obiecte conexiune. Însă nu toate serverele de chei VPN la distanţă trebuie neapărat să aibe aceleaşi proprietăţi pentru politica de date. De aceea, puteţi adăuga mai multe propuneri pentru aceeaşi politică de date. La stabilirea unei conexiuni cu un server la distanţă, trebuie să fie cel puţin o propunere corespunzătoare în politica de date a iniţiatorului şi respondentului.
   d. Apăsaţi **Adăugare** pentru a adăuga o transformare de politică de date.
   e. Selectaţi **Transport** pentru modul de încapsulare.
   f. Specificaţi o valoare pentru expirarea cheii.
   g. Apăsaţi **OK** pentru a reveni la pagina **Transformări**.
   h. Apăsaţi **OK** pentru a salva noua politică de date.
3. **Configurarea grupului de chei dinamice**

4.
   a. Din interfaţa VPN, expandaţi **Conexiuni sigure**.
   b. Faceţi clic dreapta pe **După grup** şi selectaţi **Grup nou de chei dinamice**.
   c. În pagina **General**, specificaţi un nume pentru grup. De exemplu, l2tptocorp.
   d. Selectaţi **Protejare tunel L2TP iniţiat local**.
   e. Pentru rolul sistemului, selectaţi **Ambele sisteme sunt gazde**.
   f. Mergeţi la pagina **Politică**. Selectaţi politica de date pe care aţi creat-o la pasul doi, l2tpremoteuser, din lista **Politică de date**.
   g. Selectaţi **Sistemul local iniţiază conexiunea** pentru a indica faptul că doar iSeries-A poate iniţia conexiuni cu iSeries-B.
   h. Mergeţi la pagina **Conexiuni**. Selectaţi **Generare următoarea regulă de filtrare politici pentru acest grup**. Apăsaţi **Edit** pentru a defini parametrii filtrului de politici.
   i. În pagina **Filtru de politică - Adrese locale**, selectaţi **Identificator cheie** drept tipul identificatorului.
   j. Pentru identificator, selectaţi identificatorul de cheie, thisisthekeyid, pe care l-aţi definit în politica IKE.
   k. Mergeţi la pagina **Filtru politică - Adrese la distanţă**. Selectaţi **Adresă IP Versiunea 4** din lista **Tip identificator**.
   l. Introduceţi 205.13.237.6 în câmpul **Identificator**.
   m. Mergeţi la pagina **Filtru politică - Servicii**. Introduceţi 1701 în câmpurile **Port local** şi **Port la distanţă**. Portul 1701 este binecunoscutul port pentru L2TP.
   n. Selectaţi **UDP** din lista **Protocol**.
   o. Apăsaţi **OK** pentru a reveni la pagina **Conexiuni**.
   p. Mergeţi la pagina **Interfeţe**. Selectaţi orice profil linie sau PPP pentru care se va aplica acest grup. Încă nu aţi creat profilul PPP pentru acest grup. După ce faceţi acest lucru, va trebui să editaţi proprietăţile acestui grup astfel încât grupul să se aplice pentru profilul PPP pe care îl creaţi în pasul următor.
   q. Apăsaţi **OK** pentru a crea grupul de chei dinamice, l2tptocorp.

   Acum trebuie să adăugeţi o conexiune cu grupul pe care tocmai l-aţi creat.

5. **Configurarea conexiunii cu chei dinamice**
   a. Din interfaţa VPN, expandaţi **După drup**. Aceasta afişează o listă cu toate grupurile de chei dinamice pe care le-aţi configurat pe iSeries-A.
   b. Faceţi clic dreapta pe **l2tptocorp** şi selectaţi **Conexiune nouă cu chei dinamice**.
   c. În pagina **General**, specificaţi o descriere opţională a conexiunii.
   d. Pentru serverul de chei la distanţă, selectaţi **Adresă IP v4** pentru tipul identificatorului.
   e. Selectaţi 205.13.237.6 din lista **Adresa IP**.
   f. Deselectaţi **Pornire la-cerere**.
   g. Mergeţi la pagina **Adrese locale**. Selectaţi **Identificator cheie** pentru tipul identificatorului şi apoi selectaţi thisisthekeyid din lista **Identificator**.
   h. Mergeţi la pagina **Adrese la distanţă**. Selectaţi **Adresă IP Versiunea 4** pentru tipul identificatorului.
   i. Introduceţi 205.13.237.6 în câmpul **Identificator**.
   j. Mergeţi la pagina **Servicii**. Introduceţi 1701 în câmpurile **Port local** şi **Port la distanţă**. Portul 1701 este binecunoscutul port pentru L2TP.
   k. Selectaţi **UDP** din lista **Protocol**.
   l. Apăsaţi **OK** pentru a crea conexiunea cu cheie dinamică.

Aţi terminat de configurat VPN pe iSeries-A. Următorul pas este să configuraţi un profil PPP pentru iSeries-A.

Pasul 2: Configuraţi un profil de conexiune PPP şi o linie virtuală pe iSeries-A

Această secţiune descrie paşii pe care trebuie să-i urmaţi pentru a crea profilul PPP pentru iSeries-A. Profilul PPP nu are o linie fizică asociată cu el; el foloseşte o linie virtuală. Aceasta deoarece traficul PPP tunelează prin tunelul L2TP, în timp ce VPN protejează tunelul L2TP.

Urmaţi aceşti paşi pentru a crea un profil de conexiune PPP pentru iSeries-A:

1. În Navigator iSeries, expandaţi iSeries-A **—>Reţea—>Servicii de acces la distanţă**.
2. Faceţi clic dreapta pe **Profiluri de conexiune iniţiator** şi selectaţi **Profil nou**.
3. În pagina **Setare**, selectaţi **PPP** pentru tipul protocolului.
4. Pentru Selecţii mod, selectaţi **L2TP (linie virtuală)**.
5. Selectaţi **Iniţiator la-cerere (tunel voluntar)** din lista derulantă **Mod operare**.
6. Apăsaţi **OK** pentru a merge la pagina cu proprietăţi profiluri PPP.
7. În pagina **General**, introduceţi un nume care identifică tipul şi destinaţia conexiunii. În acest caz, introduceţi toCORP. Numele trebuie pe care îl specificaţi trebuie să fie de 10 caractere sau mai puţin.
8. (opţional) Specificaţi o descriere pentru profil.
9. Mergeţi la pagina **Conexiune**.
10. În câmpul **Nume linie virtuală**, selectaţi **tocorp** din lista derulantă. Ţineţi minte că această linie nu are interfeţe fizice asociate. Linia virtuală descrie diferite caracteristici ale acestui profil PPP; de exemplu, dimensiunea maximă a cadrului, informaţii despre autentificare, nume gazdă local etc. Apare caseta de dialog **Proprietăţi linie L2TP**.
11. În pagina **General**, introduceţi o descriere pentru linia virtuală.
12. Mergeţi la pagina **Autentificare**.
13. În câmpul **Nume gazdă locală**, introduceţi numele de gazdă al serverului local de chei, iSeriesA.
14. Apăsaţi **OK** pentru a salva descrierea liniei virtuale noi şi reveniţi la pagina **Conexiune**.
15. Introduceţi adresa punctului final al tunelului de la distanţă, 205.13.237.6, în câmpul **Adresă punct final tunel la distanţă**.
16. Selectaţi **Este necesară protecţia IPSec** şi selectaţi grupul de chei dinamice pe care l-aţi creat la pasul unu, l2tptocorp din lista derulantă **Nume grup conexiune**.
17. Mergeţi la pagina **Setări TCP/IP**.
18. În secţiunea **Adresă IP locală**, selectaţi **Atribuită de sistem de la distanţă**.
19. În secţiunea **Adresă IP la distanţă**, selectaţi **Folosire adresă IP fixă**. Introduceţi 10.6.11.1, care este adresa IP a sistemului de la distanţă din subreţeaua sa.
20. În secţiunea de rutare, selectaţi **Definire rute statice suplimentare** şi apăsaţi **Rute**. Dacă nu este furnizată nici o informaţie de rutare în profilul PPP, atunci iSeries-A poate să ajungă doar la punctul final al tunelului de la distanţă, dar la nici un alt sistem de pe subreţeaua 10.6.0.0.
21. Apăsaţi **Adăugare** pentru a adăuga o intrare de rută statică.
22. Introduceţi subreţeaua, 10.6.0.0 şi masca subreţelei, 255.255.0.0 pentru a ruta tot traficul 10.6.*.* prin tunelul L2TP.
23. Apăsaţi **OK** pentru a adăuga ruta statică.
24. Faceţi clic pe **OK** pentru a închide caseta de dialog Rutare.
25. Mergeţi la pagina **Autentificare** pentru a seta numele utilizatorului şi parola pentru acest profil PPP.
26. În secţiunea Identificare sistem local, selectaţi **Permitere sistemului de la distanţă să verifice identitatea acestui sistem**.
27. Sub **Protocol de autentificare de folosit** selectaţi **Este necesară parolă criptată (CHAP-MD5)**
28. Introduceţi numele utilizatorului, iSeriesA, şi o parolă.
29. Apăsaţi **OK** pentru a salva profilul PPP.

Pasul 3: Aplicaţi grupul de chei dinamice l2tptocorp la profilul PPP toCorp

După ce aţi configurat profilul de conexiune PPP, trebuie să mergeţi înapoi la grupul de chei dinamice, l2tptocorp, pe care l-aţi creat şi să îl asociaţi cu profilul PPP. Pentru aceasta, parcurgeţi paşii următori:

1. Navigaţi la interfaţa VPN, apoi expandaţi **Conexiuni sigure —>După grup**.
2. Faceţi clic dreapta pe grupul de chei dinamice, l2tptocorp, şi selectaţi **Proprietăţi**.
3. Mergeţi la pagina **Interfeţe** şi selectaţi **Aplicare acest grup** pentru profilul PPP pe care l-aţi creat în pasul doi, toCorp.
4. Apăsaţi **OK** pentru a aplica l2tptocorp la profilul PPP, toCorp.

Pasul 4: Configuraţi VPN-ul pe iSeries-B

Urmaţi aceiaşi paşi pe care i-aţi utilizat pentru a configura iSeries-A, înlocuind adresele IP şi identificatorii după cum este cazul. Luaţi în calcul şi aceste puncte înainte să începeţi:

- Identificaţi serverul de chei la distanţă prin identificatorul cheie pe care l-aţi specificat pentru serverul de chei local pe iSeries-A. De exemplu, thisisthekeyid.
- Folosiţi *exact* aceeaşi cheie prepartajată.
- Asiguraţi-vă că transformările dumneavoastră corespund cu cele pe care le-aţi configurat pe iSeries-A sau conexiunile vor eşua.
- Nu specificaţi **Protejare tunel L2TP iniţiat local** pe pagina **General** a grupului de chei dinamice.
- Sistemul la distanţă iniţiază conexiunea.
- Specificaţi pornirea la cerere a conexiunii.

Pasul 5: Configuraţi un profil de conexiune PPP şi o linie virtuală pe iSeries-B

Urmaţi aceşti paşi pentru a crea un profil de conexiune PPP pentru iSeries-B:

1. În Navigator iSeries, expandaţi iSeries-B **—>Reţea—> Servicii de acces la distanţă**.
2. Faceţi clic dreapta pe **Profiluri de conexiune respondent** şi selectaţi **Profil nou**.
3. În pagina **Setare**, selectaţi **PPP** pentru tipul protocolului.
4. Pentru Selecţii mod, selectaţi **L2TP (linie virtuală)**.
5. Selectaţi **Terminator (server de reţea)** din lista **Modul de operare**.
6. Apăsaţi **OK** pentru pagina Proprietăţi profiluri PPP.
7. În pagina **General**, introduceţi un nume care identifică tipul şi destinaţia conexiunii. În acest caz, introduceţi tobranch. Numele trebuie pe care îl specificaţi trebuie să fie de 10 caractere sau mai puţin.
8. (opţional) Specificaţi o descriere pentru profil.
9. Mergeţi la pagina **Conexiune**.
10. Selectaţi adresa IP a punctului final local al tunelului, 205.13.237.6.
11. În câmpul **Nume linie virtuală**, selectaţi **tobranch** din lista derulantă. Ţineţi minte că această linie nu are interfeţe fizice asociate. Linia virtuală descrie diferite caracteristici ale acestui profil PPP; de exemplu, dimensiunea maximă a cadrului, informaţii despre autentificare, nume gazdă local etc. Apare caseta de dialog **Proprietăţi linie L2TP**.
12. În pagina **General**, introduceţi o descriere pentru linia virtuală.
13. Mergeţi la pagina **Autentificare**.
14. În câmpul **Nume gazdă locală**, introduceţi numele de gazdă al serverului local de chei, iSeriesB.
15. Apăsaţi **OK** pentru a salva descrierea liniei virtuale noi şi reveniţi la pagina **Conexiune**.
16. Mergeţi la pagina **Setări TCP/IP**.
17. În secţiunea **Adresă IP locală**, selectaţi adresa IP fixă a sistemului local, 10.6.11.1.
18. În secţiunea **Adresă IP la distanţă**, selectaţi **Pool de adrese** ca metodă de atribuire a adresei. Introduceţi o adresă de pornire şi apoi specificaţi numărul de adrese care pot să fie atribuite sistemului la distanţă.
19. Selectaţi **Permitere sistemului de la distanţă să acceseze alte reţele (înaintare IP)**.
20. Mergeţi la pagina **Autentificare** pentru a seta numele utilizatorului şi parola pentru acest profil PPP.
21. În secţiunea Identificare sistem local, selectaţi **Permitere sistemului de la distanţă să verifice identitatea acestui sistem**. Aceasta deschide caseta de dialog **Identificare sistem local**.

22. Sub **Protocol de autentificare de folosit** selectaţi **Este necesară parolă criptată (CHAP-MD5)**
23. Introduceţi numele utilizatorului, iSeriesB, şi o parolă.
24. Apăsaţi **OK** pentru a salva profilul PPP.

Pasul 6: Activaţi regulile pachet

VPN creează automat regulile pachet pe care le cere această conexiune pentru a funcţiona corespunzător. Oricum, trebuie să le activaţi pe ambele sisteme înainte de a porni conexiunea VPN. Pentru a face acest lucru pe iSeries-A, parcurgeţi paşii următori:

1. În Navigator iSeries, expandaţi **iSeries-A —>Reţea —>Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachete** şi selectaţi **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectaţi dacă vreţi să activaţi doar regulile generate VPN, doar un fişier selectat sau ambele variante. Puteţi alege ultima variantă, de exemplu, dacă aveţi diverse reguli PERMITERE şi REFUZARE pe care doriţi să le impuneţi pe interfaţă în plus faţă de regulile generate VPN.
4. Selectaţi interfaţa pe care vreţi să activaţi regulile. În acest caz, selectaţi **Toate interfeţele**.
5. Faceţi clic pe **OK** în caseta de dialog pentru a confirma ca vreţi să verificaţi şi să activaţi regulile pe interfaţa sau interfeţele specificate. După ce aţi apăsat OK, sistemul verifică regulile de erori sintactice şi semantice şi raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fişier anume şi un număr de linie, puteţi apăsa clic dreapta pe eroare şi selecta **Mergi la linie** pentru a evidenţia eroarea în fişier.
6. Repetaţi aceşti paşi pentru a activa regulile de pachete pe iSeries-B.

Pasul 7: Porniţi conexiunea

Pasul final este să porniţi conexiunea. Înainte să puteţi iniţia o conexiune L2TP, trebuie să activaţi terminatorul L2TP să răspundă la cererile iniţiatorului. După ce sunteţi sigur că toate serviciile cerute sunt pornite, porniţi conexiunea PPP pe partea terminatorului. Următorii paşi descriu cum să porniţi conexiunea PPP pe iSeries-B:

1. În Navigator iSeries, expandaţi **—> Reţea —> Servicii acces la distanţă** pentru iSeries-B.
2. Faceţi clic pe **Profiluri conexiune respondent** pentru a afişa o listă cu profiluri de respondent în panoul din dreapta.
3. Faceţi clic dreapta pe tobranch şi selectaţi **Pornire**. După ce profilul de conexiune porneşte, fereastra se reîmprospătează şi arată conexiunea ca În aşteptare cereri conexiune. iSeries-A poate acum să răspundă la cereri conexiune L2TP de la iSeries-B.

Urmaţi aceşti paşi pentru a porni conexiunea L2TP pe iSeries-A:

1. În Navigator iSeries, expandaţi **—> Reţea —> Servicii acces la distanţă** pentru iSeries-A.
2. Apăsaţi **Profiluri conexiune iniţiator** pentru a afişa o listă cu profiluri de respondent în panoul din dreapta.
3. Faceţi clic dreapta pe **toCORP** şi selectaţi **Pornire**. După ce profilul de conexiune porneşte, fereastră se reîmprospătează şi arată conexiunea ca Stabilind tunelul L2TP.
4. Apăsaţi F5 pentru a reîmprospăta ecranul. Dacă tunelul L2TP a pornit cu succes, starea conexiunii va fi acum Conexiuni active.

Scenariu VPN: Folosirea translatării adreselor de reţea pentru VPN

Să presupunem că dumneavoastră sunteţi administratorul de reţea pentru o companie producătoare mică din Minneapolis. Unul dintre partenerii dumneavoastră de afaceri, un furnizor de subansambluri din Chicago, vrea să înceapă să facă mai multe afaceri cu compania dumneavoastră prin Internet. Este critic pentru compania dumneavoastră să aibă anumite componente şi cantităţi exact atunci când are nevoie de ele, astfel încât furnizorul trebuie să cunoască starea inventarului companiei dumneavoastră şi de planificarea producţiei. În prezent, efectuaţi această interacţiune manual, dar constataţi că este mare consumatoare de timp, implică un cost ridicat şi uneori apar date eronate, astfel încât sunteţi mai mult decât doritor să investigaţi opţiunile pe care le aveţi.

Dată fiind natura confidenţială şi dependentă de timp a informaţiilor pe care le schimbaţi, vă decideţi să creaţi o reţea privată virtuală (VPN) între reţeaua furnizorului dumneavoastră şi reţeaua companiei dumneavoastră. Pentru a proteja şi mai mult intimitatea structurii reţelei companiei dumneavoastră, decideţi că este nevoie să ascundeţi adresa IP privată a iSeries(TM) care găzduieşte aplicaţiile la care furnizorul are acces. Întrebarea este: Cum faceţi acest lucru posibil?

Răspunsul: VPN-ul(R) OS/400. Folosiţi-l nu numai pentru a crea definiţiile conexiunilor pe gateway-ul VPN din reţeaua companiei dumneavoastră, ci şi pentru a furniza translatarea de adrese de care aveţi nevoie pentru a ascunde adresele dumneavoastră locale private. Spre deosebire de translatarea adreselor de reţea (network address translation - NAT) convenţională, care modifică adresele IP din asocierile de securitate (security associations - SAs) de care are nevoie VPN pentru a funcţiona, VPN NAT efectuează translatarea adreselor înainte de validarea SA, prin atribuirea unei adrese conexiunii în momentul în care aceasta este pornită.

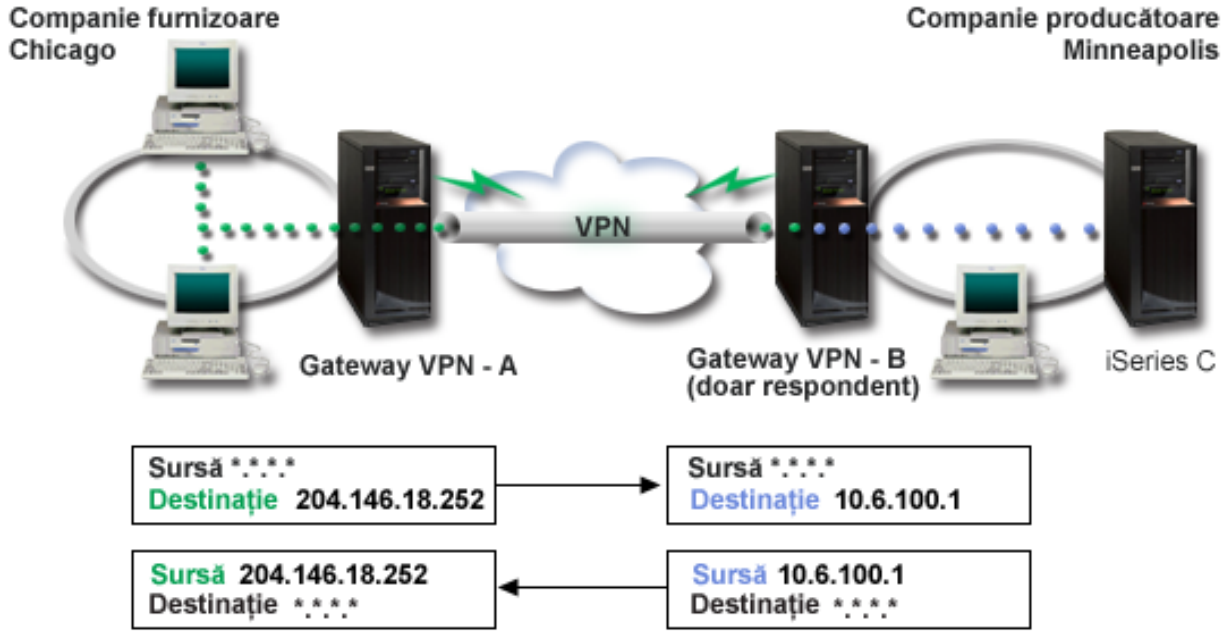
Obiective

Obiectivele acestui scenariu sunt:

- să se permită tuturor clienţilor din reţeaua furnizorului să acceseze o singură gazdă iSeries din reţeaua producătorului printr-o conexiune VPN gateway-la-gateway.
- să se ascundă adresa IP privată a iSeries-ului din reţeaua producătorului, prin translatarea acesteia într-o adresă IP publică folosind translatarea adreselor de reţea pentru VPN (VPN NAT).

Detalii

Următoarea diagramă ilustrează caracteristicile reţelei atât pentru reţeaua furnizorului , cât şi pentru reţeaua producătorului:



- VPN gateway-A este configurat pentru a iniţia întotdeauna conexiuni cu VPN gateway-B.
- VPN gateway-A defineşte capătul destinaţie pentru conexiune ca 204.146.18.252 (adresa publică atribuită lui iSeries-C).
- iSeries-C are adresa IP privată 10.6.100.1 în reţeaua producătorului.
- O adresă publică 204.146.18.252 a fost definită în pool-ul de serviciu local de pe VPN gateway-B pentru adresa privată a iSeries-C, 10.6.100.1.
- VPN gateway-B translatează adresa publică a iSeries-C în adresa privată a acestuia, 10.6.100.1, pentru datagramele de intrare. VPN gateway-B translatează datagramele răspuns, de ieşire, din 10.6.100.1 înapoi în adresa publică a iSeries-C, 204.146.18.252. Din punctul de vedere al clienţilor din reţeaua furnizorului, iSeries-C are o adresă IP de 204.146.18.252. Ei nu îşi vor da seama că s-a produs o translaţie a adresei.

Operaţii de configurare

Trebuie să efectuaţi fiecare dintre următoarele sarcini pentru a configura conexiunea descrisă în acest scenariu:

1. Configuraţi un VPN gateway-la-gateway între **VPN gateway-A** şi **VPN gateway-B**.
2. Definiţi un pool de serviciu local pe **VPN gateway-B** pentru a ascunde adresa IP privată a lui **iSeries-C** în spatele unui identificator public, 204.146.18.252.
3. Configuraţi **VPN gateway-B** pentru a translata adresele locale folosind adresele din pool-ul de serviciu local.

Conceptele VPN

Reţeaua privată virtuală (VPN) foloseşte mai multe protocoale TCP/IP importante pentru a proteja traficul de date. Pentru a înţelege mai bine cum funcţionează o conexiune VPN, familiarizaţi-vă cu aceste protocoale şi concepte şi cu felul în care le foloseşte VPN(R) OS/400:

- **Protocoale IP Security (IPSec)**
  IPSec oferă o bază stabilă şi durabilă pentru furnizarea de securitate la nivelul reţea.
- **Gestionarea cheilor**
  Un VPN dinamic furnizează securitate suplimentară pentru comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.
- **Layer 2 Tunneling Protocol (L2TP)**
  Dacă intenţionaţi să folosiţi o conexiune VPN pentru a securiza comunicaţiile dintre reţeaua dumneavoastră şi clienţii la distanţă, trebuie de asemenea să fiţi familiariazit cu L2TP.
- **Translatarea adreselor de reţea pentru VPN (VPN NAT)**
  OS/400 VPN furnizează un mijloc pentru efectuarea de translatare a adreselor de reţea, denumit VPN NAT. VPN NAT diferă de NAT tradiţional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE şi IPSec. Studiaţi acest subiect pentru a afla mai multe.
- **Încapsularea UDP**
  Încapsularea UDP permite traficului IPSec să treacă printr-un dispozitiv NAT convenţional. Treceţi în revistă acest subiect pentru mai multe informaţii despre ce este şi de ce ar trebui să îl folosiţi pentru conexiunile dumneavoastră VPN.
- **Comprimarea IP (IPComp)**
  IPComp reduce dimensiunea datagramelor IP prin comprimarea datagramelor pentru a creşte performanţele comunicaţiilor dintre doi parteneri VPN.
- **VPN şi filtrarea IP**
  Filtrarea IP şi VPN sunt foarte înrudite. De fapt, majoritatea conexiunilor VPN necesită reguli de filtrare pentru a funcţiona corect. Acest subiect vă oferă informaţii despre ce filtre necesită VPN, împreună cu alte concepte de filtrare înrudite cu VPN.

Protocoalele IP Security (IPSec)

IPSec furnizează o bază stabilă şi durabilă pentru securitatea stratului de reţea. El suportă toţi algoritmii de criptare folosiţi în prezent şi poate de asemenea îngloba algoritmi noi şi mai puternici pe măsură ce aceştia apar. Protocoalele IPSec tratează aceste probleme majore de securitate:

Autentificarea originii datelor
Verifică dacă fiecare datagramă a fost lansată de emiţătorul declarat.

Integritatea datelor
Verifică dacă datagramele au fost modificate în tranzit, deliberat sau datorită unor erori aleatoare.

Confidenţialitatea datelor
Ascunde conţinutul unui mesaj, de obicei prin criptare.

Protecţia la redare
Asigură că un atacator nu poate intercepta o datagramă pentru a o reda ulterior.

Gestionarea automată a cheilor criptografice şi a asociaţiilor de securitate
Asiguraţi-vă că politica dumneavoastră VPN poate fi utilizată prin reţeaua extinsă cu o configuraţie manuală redusă sau chiar fără.

VPN foloseşte două protocoale IPSec pentru a proteja datele care trec prin VPN: Authentication Header (AH) şi Encapsulating Security Payload (ESP). Cealaltă parte a activării IPSec este protocolul IKE (Internet Key Exchange) sau gestionarea cheilor. În timp ce IPSec vă criptează datele, IKE suportă negocierea automată a asocierilor de securitate (SA-uri) şi generarea şi reîmprospătarea automată a cheilor de securitate.

Principalele protocoale IPSec sunt listate mai jos:

- **Protocolul Authentication Header (AH)**
- **Protocolul Encapsulating Security Payload (ESP)**
- **Combinarea protocoalelor AH şi ESP**
- **Protocoalele Internet Key Exchange (IKE)**

Internet Engineering Task Force (IETF) defineşte formal IPSec în RFC 2401, *Security Architecture for the Internet Protocol*. Puteţi vedea acest RFC pe Internet la următorul sit Web: http://www.rfc-editor.org

.

Authentication Header

Protocolul Authentication Header (AH) furnizează autentificarea originii datelor, integritatea datelor şi protecţie la redare. Totuşi, AH nu oferă confidenţialitatea datelor, ceea ce înseamnă că toate datele dumneavoastră sunt trimise transparent.

AH asigură integritatea datelor cu suma de control pe care o generează un cod de autentificare mesaj, cum este MD5. Pentru a asigura autentificarea originii datelor, AH include o cheie partajată secretă în algoritmul pe care îl foloseşte pentru autentificare. Pentru a asigura protecţia la redare, AH foloseşte un câmp de numere de ordine din cadrul antetului AH. Trebuie menţionat că aceste trei funcţii diferite sunt deseori grupate şi numite **autentificare**. În cei mai simpli termeni, AH asigură că nu s-a umblat la datele dumneavoastră pe drumul lor până la destinaţia finală.

Deşi AH autentifică cât mai mult din datagrama IP, valorile anumitor câmpuri din antetul IP nu pot fi prezise de receptor. AH nu protejează aceste câmpuri, cunoscute drept câmpuri **variabile**. Totuşi, AH întotdeauna protejează conţinutul pachetului IP.

Internet Engineering Task Force (IETF) defineşte formal AH în Request for Comment (RFC) 2402, *IP Authentication Header*. Puteţi vedea acest RFC pe Internet la următorul sit Web: http://www.rfc-editor.org

.

Moduri de folosire a AH

Puteţi aplica AH în două moduri: modul transport sau modul tunel. În modul transport, antetul IP al datagramei este cel mai exterior antet IP, urmat de antetul AH şi apoi de conţinutul datagramei. AH autentifică întreaga datagramă, cu excepţia câmpurilor variabile. Totuşi, informaţiile conţinute în datagramă sunt transportate transparent şi pot fi, astfel, spionate. Modul transport necesită mai puţină procesare suplimentară decât modul tunel, dar nu oferă la fel de multă securitate.

Modul tunel creează un nou antet IP şi îl foloseşte drept cel mai exterior antet IP al datagramei. Antetul AH urmează noul antet IP. Datagrama originală (antetul IP şi conţinutul original) vin ultimele. AH autentifică întreaga datagramă, ceea ce înseamnă că sistemul care răspunde poate detecta dacă datagrama s-a schimbat în timp ce era transportată.

Când unul dintre capetele unei asocieri de securitate este un gateway, folosiţi modul tunel. În modul tunel adresele sursă şi destinaţie din cel mai exterior antet IP nu trebuie să fie la fel ca acelea din antetul IP original. De exemplu, două porţi de securitate pot funcţiona cu un tunel AH pentru a autentifica tot traficul dintre reţelele pe care le conectează împreună. De fapt, aceasta este o configurare foarte comună.

Principalul avantaj în folosirea modului tunel este că modul tunel protejează total datagrama IP încapsulată. În plus, modul tunel face posibil să folosiţi adrese private.

De ce AH?
În multe cazuri, datele dumneavoastră necesită doar autentificare. În timp ce protocolul Encapsulating Security Payload (ESP) poate realiza autentificarea, AH nu afectează performanţele sistemului dumneavoastră aşa cum face ESP. Alt avantaj al folosirii AH, este că AH autentifică întreaga datagramă. ESP, totuşi, nu autentifică antetul IP din frunte sau orice alte informaţii care apar înainte de antetul ESP.

În plus, ESP necesită algoritmi de criptare puternici pentru a putea fi pus în practică. Criptografia puternică este restricţionată în unele ţări, în timp ce AH poate fi folosit liber în întreaga lume.

Ce algoritmi foloseşte AH pentru a-mi proteja informaţiile?
AH foloseşte algoritmi cunoscuţi drept **coduri hash de autentificare mesaje (HMAC)**. În mod specific, VPN foloseşte fie HMAC-MD5 fie HMAC-SHA. Atât MD5 , cât şi SHA folosesc date de intrare de lungime variabilă şi o cheie secretă pentru a produce date de ieşire de lungime fixă (numită valoare hash). Dacă valorile hash ale unor mesaje coincid, este foarte probabil ca mesajele sa fie identice. Atât MD5 , cât şi SHA criptează lungimea mesajului la ieşire, dar SHA este considerat mai sigur deoarece produce hash-uri mai mari.

Internet Engineering Task Force (IETF) defineşte formal HMAC-MD5 în RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Internet Engineering Task Force (IETF) defineşte formal HMAC-SHA în RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Puteţi vedea aceste RFC-uri pe Internet la următorul sit Web: http://www.rfc-editor.org

.

Encapsulating Security Payload

Protocolul Encapsulating Security Payload (ESP) furnizează confidenţialitatea datelor şi, opţional, autentificarea originii datelor, verificarea integrităţii datelor şi protecţie la redare. Diferenţa dintre ESP şi protocolul Authentication Header (AH) constă în faptul că ESP furnizează criptare, în timp de ambele protocoale furnizează autentificare, verificare de integritate şi pretecţie la redare. Cu ESP, ambele sisteme care comunică folosesc o cheie partajată pentru criptarea şi decriptarea datelor schimbate.

Dacă vă decideţi să folosiţi atât criptare , cât şi autentificare, sistemul care răspunde mai întâi autentifică pachetul şi apoi, dacă primul pas reuşeşte, sistemul continuă cu decriptarea. Acest tip de configuraţie reduce procesarea suplimentară şi vulnerabilitatea la atacuri prin negarea-serviciilor.

Două moduri de a folosi ESP
Puteţi folosi ESP în două moduri: modul transport şi modul tunel. În modul transport, antetul ESP urmează antetul IP al datagramei IP originale. Dacă datagrama are deja un antet IPSec, atunci antetul ESP vine înaintea lui. Trailer-ul ESP şi datele opţionale de autentificare urmează după încărcătura utilă.

Modul transport nu autentifică sau criptează antetul IP, ceea ce ar putea expune informaţiile dumneavoastră de adresă unor potenţiali atacatori în timp ce datagrama este în tanzit. Modul transport necesită mai puţină procesare suplimentară decât modul tunel, dar nu oferă la fel de multă securitate. În cele mai multe cazuri, gazdele folosesc ESP în modul transport.

Modul tunel creează un nou pachet IP şi îl foloseşte ca antet IP exterior al datagramei, urmat de antetul ESP şi apoi de datagrama originală (atât antetul IP , cât şi încărcătura originală). Trailer-ul ESP şi datele opţionale de autentificare sunt ataşate la încăcătură. Când folosiţi atât criptare , cât şi autentificare, ESP protejează complet datagrama originală deoarece aceasta este acum încăcătura pentru noul pachet ESP. ESP nu protejează totuşi noul antet IP. Gateway-urile trebuie să folosească ESP în modul tunel.

Ce algoritmi foloseşteESP pentru a proteja informaţiile
ESP foloseşte o cheie simetrică, cu care ambele părţi criptează şi decriptează datele pe care le schimbă. Transmiţătorul

şi receptorul trebuie să se înţeleagă asupra cheii înainte de a putea comunica în siguranţă. VPN OS/400(R) utilizează DES (Data Encryption Standard), 3DES (triple-DES), RC5, RC4 şi AES (Advanced Encryption Standard) pentru criptare.

Internet Engineering Task Force (IETF) defineşte formal DES în RFC 1829, *The ESP DES-CBC Transform*. Internet Engineering Task Force (IETF) defineşte formal 3DES în RFC 1851, *The ESP Triple DES Transform*. Puteţi vedea aceste RFC-uri şi altele pe Internet la următoarea adresă Web: http://www.rfc-editor.org

.

ESP foloseşte algoritmii HMAC-MD5 şi HMAC-SHA pentru a furniza funcţii de autentificare. Atât MD5 , cât şi SHA folosesc date de intrare de lungime variabilă şi o cheie secretă pentru a produce date de ieşire de lungime fixă (numită valoare hash). Dacă valorile hash ale unor mesaje coincid, este foarte probabil ca mesajele sa fie identice. Atât MD5 , cât şi SHA criptează lungimea mesajului la ieşire, dar SHA este considerat mai sigur deoarece produce hash-uri mai mari.

Internet Engineering Task Force (IETF) defineşte formal HMAC-MD5 în RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Internet Engineering Task Force (IETF) defineşte formal HMAC-SHA în RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Puteţi vedea aceste RFC-uri şi altele pe Internet la următoarea adresă Web: http://www.rfc-editor.org

.

AH şi ESP combinate

VPN vă permite să combinaţi AH şi ESP pentru conexiuni gazdă-la-gazdă în modul transport. Combinarea acestor protocoale protejează întreaga datagramă IP. Deşi combinarea celor două protocoale oferă mai multă securitate, procesarea suplimentară pe care o implică poate să depăşească beneficiile.

Gestionarea cheilor

Cu fiecare negociere cu succes, serverele VPN regenerează cheile care protejează o conexiune, făcând astfel mult mai dificilă pentru un atacator capturarea informaţiilor din conexiune. În plus, dacă folosiţi secretul perfect al înaintării (perfect forward secrecy), atacatorii nu pot deriva cheile viitoare pe baza informaţiilor despre cheile vechi.

Managerul de chei VPN este implementarea IBM(TM)s a protocolului Internet Key Exchange (IKE). Managerul de chei suportă negocierea automată a asocierilor de securitate (security association - SA), ca şi generarea şi reîmprospătarea automată a cheilor criptografice.

O **asociere de securitate (SA)** conţine informaţii care sunt necesare pentru a folosi protocoale IPSec. De exemplu, o SA identifică tipurile de algoritmi, lungimile şi duratele de viaţă ale cheilor, părţile participante şi modurile de încapsulare.

Cheile criptografice, după cum implică şi numele, blochează, sau protejează, informaţiile dumneavoastră până când ajunge în siguranţă la destinaţia ei finală.

Notă: Generarea în siguranţă a cheilor este cel mai important factor în stabilirea unei conexiuni sigure şi private. Dacă sunt compromise cheile dumneavoastră, atunci eforturile dumneavoastră de autentificare şi criptare, oricât de puternice, devin inutile.

Fazele gestionării cheilor

Managerul de chei VPN foloseşte două faze distincte în implementare.

Faza 1
Faza 1 stabileşte o cheie secretă principală din care sunt derivate toate cheile criptografice următoare pentru a

proteja traficul de date al utilizatorului. Aceast lucru este adevărat chiar dacă încă nu există nici o protecţie de securitate între cele două capete. VPN foloseşte ori modul semnătură RSA, ori chei prepartajate pentru a autentifica negocierile din faza 1, ca şi pentru a stabili cheile care protejează mesajele IKE care circulă în timpul negocierilor din faza 2.

O *cheie prepartajată* este un şir de caractere neobişnuite, de până la 128 caractere lungime. Ambele capete ale conexiunii trebuie să fie de acord cu cheia prepartajată. Avantajul folosirii cheilor prepartajate este simplitatea lor, dezavantajul este că un secret partajat trebuie să fie distribuit afară-din-bandă, de exemplu prin telefon sau prin poştă înregistrată, înaintea negocierilor IKE. Trataţi cheia prepartajată ca pe o parolă.

Autentificarea cu *Semnătură RSA* oferă o securitate mai mare decât cheile prepartajate deoarece acest mod foloseşte certificate digitale pentru a furniza autentificarea. Trebuie să vă configuraţi certificatele digitale folosind Digital Certificate Manager (5722-SS1 Opţiunea 34). În plus, unele soluţii VPN necesită Semnături RSA pentru interoperabilitate. De exemplu, VPN Windows(R) 2000 utilizează Semnătura RSA ca metodă implicită de autentificare. În fine, RSA Signature oferă mai multă scalabilitate decât cheile partajate. Certificatele pe care le folosiţi trebuie să provină de la autorităţi de certificare în care au încredere ambele servere.

Faza 2
Faza 2 negociază însă asocierile şi cheile de securitate care protejează schimburile reale de date ale aplicaţiei. Reţineţi că, până în acest punct, nu au fost trimise nici un fel de date ale aplicaţiei. Faza 1 protejează mesajele IKE ale fazei 2.

După ce negocierile fazei 2 sunt încheiate, VPN stabileşte o conexiune sigură, dinamică, peste reţea şi între capetele pe care le definiţi pentru conexiunea dumneavoastră. Toate datele care circulă prin VPN sunt livrate cu un grad de securitate şi eficienţă asupra căruia serverele cheie au căzut de acord în timpul proceselor de negociere din faza 1 şi faza 2.

În general, negocierile din faza 1 sunt negociate o dată pe zi, în timp ce negocierile din faza 2 sunt reîmprospătate la fiecare 60 de minute sau chiar la fiecare cinci minute. Rate de reîmprospătare mai mari măresc securitatea datelor dumneavoastră, dar scad performanţa sistemelor. Folosiţi durate de viaţă scurte ale cheilor pentru a proteja datele dumneavoastră cele mai sensibile.

Când creaţi un VPN dinamic utilizând Navigator iSeries(TM), trebuie să definiţi o politică IKE pentru a activa negocierile din faza 1 şi o politică de date pentru a guverna negocierile din faza 2. În mod opţional, puteţi folosi vrăjitorul de Conexiune nouă. Vrăjitorul creează automat fiecare dintre obiectele de configurare pe care le necesită VPN pentru a funcţiona corect, inclusiv o politică IKE şi o politică de date.

Lecturi recomandate
Dacă vreţi să citiţi mai multe despre protocolul IKE (Internet Key Exchange) şi despre gestiunea cheie, revedeţi aceste cereri pentru comentarii (RFC) 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)*

Puteţi citi aceste RFC-uri pe Internet, la următorul sit Web: http://www.rfc-editor.org

.

Layer 2 Tunnel Protocol (L2TP)

Conexiunile Layer 2 Tunneling Protocol (L2TP), numite de asemenea linii virtuale, oferă acces ieftin utilizatorilor la distanţă, permiţând unui server din reţeaua unei companii să gestioneze adresele IP atribuite utilizatorilor săi la distanţă. Mai mult, conexiunile L2TP furnizează acces sigur la sistemul sau reţeaua dumneavoastră când le folosiţi împreună cu IP Security (IPSec).

L2TP suportă dou feluri de tunel: tunelul voluntar şi tunelul obligatoriu. Diferenţa majoră dintre aceste două moduri de tunel este punctul final. La tunelul voluntar, tunelul se termină la clientul la distanţă, pe când tunelul obligatoriu se termină la ISP.

Cu un **tunel obligatoriu** L2TP, o gazdă la distanţă iniţiază o conexiune cu Furnizorul său de Servicii Internet (ISP). Apoi ISP-ul stabileşte o conexiune L2TP între utilizatorul la distanţă şi reţeaua companiei. Deşi ISP stabileşte conexiunea, dumneavoastră decideţi cum să protejaţi traficul folosind VPN. Pentru un tunel obligatoriu, ISP-ul trebuie să suporte LT2P.

Cu un **tunel voluntar** L2TP, conexiunea este creată de utilizatorul la distanţă, de obicei folosind un client de tunel L2TP. Astfel, utilizatorul trimite pachete L2TP către ISP-ul său, care le înaintează către reţeaua companiei. Cu un tunel voluntar, ISP-ul nu are nevoie să suporte L2TP. Scenariul, *Protejare tunel voluntar L2TP cu IPSec* vă furnizează un exemplu despre cum să configuraţi un iSeries(TM) dintr-un birou de filială să se conecteze la reţeaua sa corporativă printr-un gateteway iSeries cu un tunel L2TP protejat de VPN.

Puteţi vedea o prezentare vizuală despre conceptul de tuneluri voluntare L2TP protejate de IPSec. Aceasta necesită plug-in-ul Flash

. Alternativ, puteţi utiliza versiunea HTML a acestei prezentări.

L2TP este de fapt o variaţie a unui protocol de încapsulare IP. Tunelul L2TP este creat prin încapsularea unui cadru L2TP într-un pachet UDP, care este la rândul lui încapsulat într-un pachet IP. Adresele sursă şi destinaţie ale acestui pachet definesc punctele finale ale conexiunii. Deoarece protocolul de încapsulare exterioară este IP, puteţi aplica protocoale IPSec la pachetul IP compus. Aceasta protejează datele care circulă în tunelul L2TP. Puteţi aplica apoi protocoalele AH, ESP şi IKE în mod direct.

Vedeţi Scenariu: Configurarea conexiunii prin apel telefonic PPP la distanţă pentru un exemplu privind modul în care se foloseşte L2TP pentru conectarea la IBM (R) prin Universal Connection.

Translatarea adreselor de reţea pentru VPN

Translatarea adreselor de reţea (Network address translation - NAT) ia adresele IP private şi le translatează în adrese publice IP. Aceasta ajută la economisirea valoroaselor adrese publice, permiţând în acelaşi timp calculatoarelor gazdă din reţeaua dumneavoastră să acceseze servicii şi gazde la distanţă de pe Internet (sau din alte reţele publice).

În plus, dacă folosiţi adrese IP private, acestea pot intra în coliziune cu adrese IP de intrare similare. De exemplu, aţi putea dori să comunicaţi cu altă reţea dar ambele reţele folosesc adrese 10.*.*.*, provocând coliziunea adreselor şi pierderea tuturor pachetelor. Aplicarea NAT asupra adreselor de ieşire ar putea părea răspunsul la această problemă. Oricum, dacă traficul de date este protejat de un VPN, translatarea NAT convenţională nu va funcţiona deoarece modifică adresele IP din asocierile de securitate (security associations - SAs) pe care le necesită VPN pentru a funcţiona. Pentru a evita această problemă, VPN oferă propria versiune de translatare a adreselor de reţea numită VPN NAT. VPN NAT efectuează translatarea adreselor înainte de validarea SA prin atribuirea unei adrese conexiunii atunci când este pornită conexiunea. Adresa rămâne asociată cu conexiunea până când ştergeţi conexiunea.

Notă: În prezent FTP nu suportă VPN NAT.

Cum ar trebui să folosesc VPN NAT?
Sunt două tipuri diferite de VPN NAT pe care trebuie să le luaţi în considerare înainte să începeţi. Acestea sunt:

VPN NAT pentru prevenirea conflictelor între adresele IP
Acest tip de VPN NAT vă permite să evitaţi posibile conflicte între adrese IP când configuraţi o conexiune VPN

între reţele sau sisteme cu scheme de adresare similare. Un scenariu tipic este cel în care ambele companii doresc să creeze conexiuni VPN prin folosirea unuia dintre intervalele de adrese IP private atribuite lor. De exemplu, 10.*.*.*. Modul în care configuraţi acest tip de VPN NAT depinde de faptul că serverul dumneavoastră este iniţiatorul conexiunii VPN sau respondent. Când serverul dumneavoastră este iniţiatorul conexiunii, puteţi translata adresele dumneavoastră locale în unele care sunt compatibile cu adresele partenerului dumneavoastră din conexiunea VPN. Când serverul dumneavoastră este cel care răspunde la deschiderea conexiunii, puteţi translata adresele la distanţă ale partenerului dumneavoastră de VPN în unele care sunt compatibile cu schema dumneavoastră locală de adresare. Configuraţi acest tip de translatare de adrese doar pentru conexiunile dumneavoastră dinamice.

VPN NAT pentru ascunderea adreselor locale
Acest tip de VPN NAT este folosit în special pentru a ascunde adresa IP reală a sistemului dumneavoastră local prin translatarea adresei acestuia în altă adresă pe care o faceţi disponibilă public. Când configuraţi VPN NAT, puteţi decide ca fiecare adresă IP cunoscută public să fie translatată într-una dintr-un set de adrese ascunse. Aceasta vă permite de asemenea să echilibraţi încărcarea traficului pentru o adresă individuală prin repartizarea mai multor adrese. VPN NAT pentru adrese locale necesită ca serverul dumneavoastră să acţioneze ca respondent la conexiuni.

Folosiţi VPN NAT pentru ascunderea adreselor locale dacă răspundeţi da la aceste întrebări:

1. Aveţi unul sau mai multe servere pe care doriţi ca oamenii să le acceseze prin utilizarea unei VPN?
2. Aveţi nevoie de flexibilitate în legătură cu adresele IP efective ale sistemelor dumneavoastră?
3. Aveţi una sau mai multe adrese IP rutabile global?

Scenariul, *Utilizare translatare adresă reţea pentru VPN* vă furnizează un exemplu de cum să configuraţi VPN NAT să ascundă adresele locale din iSeries(TM).

Pentru instrucţiuni pas-cu-pas despre cum să setaţi VPN NAT pe iSeries-ul dumneavoastră, folosiţi ajutorul online disponibil din interfaţa VPN a Navigatorului iSeries.

IPSec compatibil cu NAT

Problema: NAT-ul convenţional întrerupe VPN-ul

Translatarea adreselor de reţea (NAT) vă permite să ascundeţi adresele IP private neînregistrate în spatele unui set de adrese IP înregistrate. Aceasta vă ajută să vă protejaţi reţeaua internă de reţelele exterioare. De asemenea, NAT vă ajută în problema terminării adreselor IP, din moment ce multe adrese private pot fi reprezentate de un set mic de adrese înregistrate.

Din nefericire, NAT convenţional nu funcţionează pe pachetele IPSec, deoarece când pachetul merge printr-un dispozitiv NAT, adresa sursă din pachet se schimbă, astfel invalidând pachetul. Când se întâmplă aceasta, capătul receptor al conexiunii VPN rejectează pachetul şi negocierile conexiunii VPN eşuează.

Soluţia: Încapsularea UDP
Într-un înveliş, încapsularea UDP împachetează pachetul IPSec înăuntrul unui antet IP/UDP nou, dar duplicat. Adresa din noul antet IP este translatată când merge prin dispozitivul NAT. Apoi, când pachetul ajunge la destinaţie, capătul receptor înlătură antetul suplimentar, lăsând pachetul IPSec original, care va trece acum toate celelalte validări.

Puteţi să aplicaţi încapsularea UDP doar la VPN-uri care vor folosi IPSec ESP în modul tunel sau modul transport. În plus, la V5R2 serverul iSeries (TM) se poate comporta doar ca un client pentru încapsularea UDP. Cu late cuvinte, poate doar să *iniţieze* trafic încapsulat UDP.

Desenele de mai jos ilustrează formatul unui pachet ESP încapsulat UDP în modul tunel:

Datagrama IPv4 originală:

După aplicarea IPSec ESP în modul tunel:

După ce se aplică Încapsularea UDP:

Desenele de mai jos ilustrează formatul unui pachet ESP încapsulat UDP în modul transport:

Datagrama IPv4 originală:

După aplicarea IPSec ESP în modul transport:

După ce se aplică Încapsularea UDP:

După ce pachetul este încapsulat, iSeries îl trimite partenerului său VPN prin UDP portul 4500. Tipic, partenerii VPN realizează negocieri IKE prin UDP port 500. Totuşi, când IKE detectează NAT în timpul negocierii cheie, pachetele IKE următoare sunt trimise prin portul sursă 4500, portul destinaţie 4500. Aceasta înseamnă de asemenea că portul 4500 trebuie să nu fie restricţionat în nici o regulă filtru aplicabilă. Capătul receptor al conexiunii poate determina dacă pachetul este unul IKE sau unul încapsulat UDP deoarece primii 4 octeţi ai încărcăturii utile UDP sunt setaţi pe zero pe un pachet IKE. Pentru a funcţiona corect, ambele capete ale conexiunii trebuie să suporte încapsularea UDP.

Comprimarea IP (IPComp)

Protocolul IP Payload Compression (IPComp) reduce dimensiunea datagramelor IP comprimând datagramele pentru a creşte performanţa comunicaţiei între doi parteneri. Intenţia este să se mărească performanţa totală a comunicaţiei atunci când comunicaţia se face peste legături lente sau încăcate. IPComp nu furnizează nici un fel de securitate şi trebuie folosit cu o transformare AH sau ESP când comunicaţia are loc peste o conexiune VPN.

Internet Engineering Task Force (IETF) defineşte formal IPComp în RFC 2393, *IP Payload compression Protocol (IPComp)*. Puteţi vedea acest RFC pe Internet la urmatoarea adresă Web: http://www.rfc-editor.org

.

VPN şi filtrarea IP

Cele mai multe conexiuni VPN necesită reguli filtru pentru a funcţiona corect. Regulile de filtrare necesare depind de tipul de conexiune VPN pe care o configuraţi, ca şi de tipul ce trafic pe care doriţi să-l controlaţi. În general, fiecare conexiune va avea un filtru de politică. Filtrul de politică defineşte care adrese, protocoale şi porturi pot folosi VPN-ul. În plus, conexiunile care suportă protocolul IKE (Internet Key Exchange) au tipic reguli care sunt scrise explicit pentru a permite procesare IKE asupra conexiunii.

Începând cu ediţia V5R1 a sistemului de operare, VPN poate genera aceste reguli în mod automat. Când este posibil, permiteţi VPN-ului să genereze filtrele de politică pentru dumneavoastră. Aceasta nu va ajuta doar la eliminarea erorilor, dar elimină de asemnea şi nevoia ca dumneavoastră să configuraţi regulile ca un pas separat, folosind editorul Reguli pachet din Navigator iSeries(TM).

Desigur, sunt şi excepţii. Treceţi în revistă aceste subiecte pentru a afla mai multe despre alte concepte şi tehnici de filtrare VPN, mai puţin obişnuite, care pot fi valabile în cazul dumneavoastră:

- **Migrarea filtrelor de politici în ediţia curentă**
  În versiunile V4R4 şi V4R5 ale sistemului de operare, trebuia să configuraţi regulile pentru pachete VPN într-un pas separat. Acestea nu erau generate automat ca parte a configurării VPN. Acest subiect detaliază consideraţii speciale pentru migrarea filtrelor de politici V4R4 şi V4R5 către ediţia curentă şi vă spune cum să faceţi acest lucru.
- **Conexiunea VPN fără filtre de politică**
  În cazul în care punctele finale ale conexiunii dumneavoastră VPN sunt adrese IP specifice, singulare şi doriţi să porniţi VPN fără a fi nevoie să scrieţi sau să activaţi reguli de filtrare pe sistem, puteţi configura un filtru de politică dinamic. Acest subiect explică de ce aţi putea lua în considerare acest lucru şi vă descrie cum să îl faceţi.
- **IKE Implicit**
  Pentru a se realiza negocieri IKE pentru VPN-ul dumneavoastră, trebuie să permiteţi datagrame UDP pe portul 500 pentru acest tip de trafic IP. Oricum, dacă nu există reguli de filtrare pe sistemul dumneavoastră scrise special pentru a permite traficul IKE, atunci sistemul va permite în mod implicit fluxul traficului IKE. Citiţi acest subiect pentru informaţii suplimentare despre cum funcţionează pe un iSeries.

Migrarea filtrelor de politici la ediţia curentă

În V4R4 şi V4R5 ale sistemului de operare, trebuia să configuraţi regulile pachet VPN ca un pas separat în interfaţa Reguli pachet din Navigator iSeries(TM). Acestea nu erau generate automat ca parte a configurării VPN. Începând cu versiunea V5R1 a sistemului de operare, GUI-ul VPN poate crea automat aceste reguli de pachete.

Trebuie să ţineţi seama de câteva lucruri dacă aţi creat reguli filtrare politici (reguli în care action=IPSEC) în V4R4 sau V4R5 şi doriţi să le folosiţi în versiunea curentă. Sau poate VPN *va genera* regulile dumneavoastră de filtrare a politicilor, dar trebuie să adăugaţi reguli suplimentare care să permită alt trafic IP, de exemplu telnet, prin conexiune. Urmaţi aceste recomandări pentru a evita potenţiale erori de configurare.

Clarificare: Când acest subiect se referă la fişierul de reguli *client*, se referă la orice fişier de reguli pe care l-aţi creat folosind editorul de reguli de pachet din Navigator iSeries. Aceasta spre deosebire de fişierul de reguli *VPNPOLICYFILTERS.I3P*, care este fişierul de reguli pe care VPN îl generează automat ca parte a configurării VPN.

- Dacă aveţi conexiuni VPN şi din V4R4 şi V4R5 şi nu doriţi să configuraţi alte conexiuni VPN în ediţia curentă, puteţi activa regulile de filtrare şi porni conexiunile, ca de obicei.
- Dacă aveţi conexiuni VPN din V4R4 sau din V4R5 şi intenţionaţi să configuraţi conexiuni VPN noi în ediţia curentă, utilizaţi vrăjitorul **Migrare filtre politică**. Vrăjitorul înlătură filtrele de politici din fişierele de reguli de pachet pe care le-aţi creat şi inserează filtre de politici echivalente în fişierul VPNPOLICYFILTERS.I3P, generat de VPN. Pentru a accesa acest vrăjitor, parcurgeţi paşii următori:
  1. În Navigator iSeries, expandaţi-vă serverul —>**Reţea** —>**Politici IP**.
  2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Filtre politică de migrare**.

3. Când aţi terminat cu vrăjitorul, faceţi clic pe **Sfârşit**.
4. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.

- Dacă VPN a generat regulile dumneavoastră de filtrare a politicilor, dar trebuie să adăugaţi reguli de filtrare non-VPN, trebuie să configuraţi aceste reguli utilizând Editorul de reguli pachet din Navigator iSeries. Dacă vreuna dintre aceste reguli de filtrare non-VPN trebuie să vină înaintea filtrelor VPN, începeţi numele lor cu PREIPSEC. De exemplu PREIPSECMYRULES. Acesta ajută sistemul să detemine în ce ordine va procesa regulile dumneavoastră de filtru. Numele seturilor tuturor celorlalte reguli non-VPN nu trebuie să aibă prefixul PREIPSEC. De exemplu, MORERULES.
- Permiteţi întotdeauna VPN-ului să creeze reguli proprii de filtru politică. Totuşi, regulile dumneavoastră de filtrare non-VPN trebuie să rămână în fişierul de reguli client. Ţineţi minte, dacă vreunul din aceste filtre non-VPN trebuie să vină înainte de filtrele de politici în fişierul de reguliVPNPOLICYFILTERS.I3P, va trebui să adăugaţi PREIPSEC în faţa numelui. Aceasta asigură că regulile client şi regulile VPN funcţionează împreună corespunzător. De exemplu, VPN a generat regulile dumneavoastră de filtrare politici (seturi VPN), dar dumneavoastră aţi adăugat reguli suplimentare (Seturile dumneavoastră) pentru a permite şi alt trafic IP prin conexiune. Când încărcaţi regulile în sistem, ele vor fi ordonate după cum urmează:
  1. Seturile dumneavoastră ale căror nume încep cu PREIPSEC
  2. Seturile VPN ale căror nume încep cu PREIPSEC
  3. Seturile VPN cu ACTION=IPSEC (filtre de politici)
  4. Seturile dumneavoastră cu ACTION=IPSEC (filtre de politici)
  5. Celelalte filtre ale dumneavoastră.
  6. Celelalte filtre VPN.

  Verificaţi fişierul EXPANDED.OUT pentru a vedea ordinea fişierului de ieşire combinat. EXPANDED.OUT este scris în directorul unde este localizat fişierul de reguli client.
- Utilizând Navigatorul iSeries, puteţi alege să activaţi:
  - numai fişierul de reguli generate de VPN, VPNPOLICYFILTERS.I3P
  - numai fişierul dumneavoastră de reguli client
  - atât regulile VPN generate , cât şi fişierul dumneavoastră de reguli client
- Activaţi regulile dumneavoastră de filtrare pe toate interfeţele, mai degrabă decât pe o interfaţă individuală. Aceasta ajută la garantarea activării filtrelor şi de asemenea va seta ordinea corectă a filtrelor politici.
- Întotdeauna verificaţi-vă regulile filtru înainte de a încerca să le activaţi. Dacă verificarea rulează fără erori, verificaţi EXPANDED.OUT pentru a vă asigura că regulile sunt ordonate cum aţi intenţionat. După ce terminaţi acest pas, puteţi activa regulile.

Conexiuni VPN fără filtre de politici

O regulă de filtrare politică defineşte care adrese, protocoale şi porturi pot utiliza un VPN şi dirijează traficul corespunzător prin conexiune. În unele cazuri, aţi putea dori să configuraţi o conexiune care nu necesită o regulă de filtrare politici. De exemplu, puteţi avea reguli pentru pachete non-VPN încărcate în interfaţa pe care o va folosi conexiunea dumneavoastră VPN, astfel că, în loc să deactivaţi regulile active de pe acea interfaţă, vă decideţi să configuraţi VPN-ul astfel încât sistemul dumneavoastră să se ocupe în mod dinamic de toate filtrele pentru conexiune. Filtrul de politici pentru acest tip de conexiune este denumit **filtrul de politici dinamic**. Înainte să puteţi folosi un filtru dinamic de politici pentru conexiunea dumneavoastră VPN, trebuie să fie adevărate următoarele:

- Conexiunea poate fi iniţiată doar de către serverul local.
- Capetele de date ale conexiunii trebuie să fie sisteme singulare. Adică nu pot fi o subreţea sau un domeniu de adrese.
- Nu poate fi încărcată nici o regulă de filtrare politică pentru conexiune.

Dacă toate aceste condiţii sunt îndeplinite de conexiunea dumneavoastră, o puteţi configura astfel încât să nu necesite un filtru de politică. Atunci când se deschide conexiunea, traficul dintre punctele finale de date va circula de-a lungul ei indiferent dacă sunt încărcate în sistem alte reguli pentru pachete.

Pentru instrucţiuni pas-cu-pas despre cum să configuraţi o conexiune astfel încât să nu necesite un filtru politică, utilizaţi ajutorul online pentru VPN.

IKE Implicit

Pentru a stabili o conexiune, cele mai multe VPN-uri necesită apariţia unor negocieri IKE (Internet Key Exchange) înainte de procesarea IPSec. IKE foloseşte binecunoscutul port 500, astfel că pentru ca IKE să funcţioneze bine, trebuie să permiteţi datagramele UDP pe port 500 pentru acest tip de trafic IP. Dacă nu există reguli de filtrare special pentru permiterea traficului IKE, atunci acesta este implicit permis. Totuşi, regulile scrise specific pentru traficul portului 500 UDP sunt tratate pe baza a ceea ce e definit în regulile filtru active.

Planificarea pentru VPN

Planificarea este o parte esenţială a soluţiei dumneavoastră VPN totale. Sunt multe decizii complexe pe care trebuie să le luaţi pentru a vă asigura funcţionarea corespunzătoare a conexiunii dumneavoastră. Folosiţi aceste resurse pentru a aduna toate informaţiile de care aveţi nevoie pentru a asigura succesul VPN-ului dumneavoastră:

- **Cerinţe de instalare VPN**
  Înainte să începeţi, asiguraţi-vă că îndepliniţi cerinţele minime pentru crearea unei VPN.
- **Determinaţi ce tip de VPN să creaţi**
  Determinarea modului în care veţi folosi VPN este unul dintre primii paşi în planificarea cu succes. Acest subiect descrie diversele tipuri de conexiuni pe care le puteţi configura.
- **Folosirea consilierului de planificare VPN**
  Consilierul de planificare vă pune întrebări despre reţeaua dumneavoastră şi, pe baza răspunsurilor dumneavoastră, vă furnizează sugestii pentru crearea VPN-ului dumneavoastră.
  Notă: Folosiţi consilierul de planificare VPN doar pentru conexiunile care suportă protocolul Internet Key Exchange (IKE). Pentru conexiunile dumneavoastră manuale, folosiţi foaia de lucru pentru planificarea conexiunilor manuale.
- **Completarea foilor de lucru pentru planificarea VPN-ului**
  Dacă preferaţi, puteţi tipări şi completa foile de lucru pentru planificare, pentru a culege informaţii detaliate privind planurile de folosire a VPN-ului.

După ce aţi găsit un plan pentru VPN, puteţi începe configurarea ei.

Cerinţele pentru setarea VPN

Pentru a funcţiona corespunzător pe iSeries(TM) şi cu clienţii reţea, asiguraţi-vă că iSeries şi clientul PC îndeplinesc următoarele cerinţe:

Cerinţe V5R2 iSeries

- OS/400(R) Versiunea 5 Ediţia 2 (5722-SS1) sau mai recentă
- Digital Certificate Manager (5722-SS1 Opţiunea 34)
- Cryptographic Access Provider (5722-AC2 sau AC3)
- Acces iSeries pentru Windows(R)(5722-XE1) şi Navigator iSeries
  - Componenta de reţea a Navigatorului iSeries
- Setaţi valoarea sistem reţinere date de securitate de pe server (QRETSVRSEC *SEC) la 1.
- TCP/IP trebuie să fie configurat, inclusiv interfeţe IP, rute, nume gazdă locală şi nume domeniu local.

Cerinţe client

- O staţie de lucru cu un sistem de operare Windows(R) pe 32 de biţi, conectată corespunzător la iSeries-ul dumneavoastră şi configurată pentru TCP/IP
- O unitate de procesare la 233 MHz
- 32 MB RAM pentru clienţii Windows 95/98
- 64 MB RAM pentru clienţii Windows NT(R) şi 2000
- iSeries Access for Windows şi Navigator iSeries instalate pe PC-ul client
- Software care suportă protocolul IP Security (IPSec)
- Software care suportă L2TP, dacă utilizatorii de la distanţă vor folosi L2TP pentru a stabili o conexiune cu sistemul dumneavoastră.

Determinarea tipului de VPN ce urmează să fie creat

Determinarea modului în care veţi folosi VPN este unul dintre primii paşi în planificarea cu succes. Pentru a face aceasta, trebuie să înţelegeţi rolul pe care îl joacă pentru conexiune atât serverul de chei local, cât şi serverul de chei la distanţă. De exemplu, sunt capetele *conexiunii* diferite de capetele *datelor*? Sunt aceleaşi sau vreo combinaţie a lor? Capetele conexiunii autentifică şi criptează (sau decriptează) traficul de date pentru conexiune şi furnizează (opţional) gestionarea cheilor cu protocolul Internet Key Exchange (IKE). Puntele finale de date, totuşi, definesc conexiunea dintre două sisteme pentru traficul IP care circulă prin VPN; de exemplu, tot traficul TCP/IP dintre 123.4.5.6 şi 123.7.8.9. În mod tipic, când capetele conexiunii şi capetele datelor sunt diferite, serverul VPN este un gateway. Când sunt aceleaşi, serverul VPN este un calculator gazdă.

Urmează diverse tipuri de implementări VPN care sunt potrivite pentru nevoile majorităţii afacerilor:

Gateway-la-gateway
Capetele conexiunii de pe ambele sisteme sunt diferite de capetele datelor. Protocolul IP Security (IPSec) protejează traficul ce călătoreşte între gateway-uri. Oricum, IPSec nu protejează traficul de date din reţelele interne de pe nici una dintre părţi. Aceasta este o setare obişnuită pentru conexiunile dintre birourile filialelor deoarece traficul care este rutat dincolo de gateway-urile birourilor filialelor, către reţelele interne, este adeseori considerat de încredere.

Gateway-la-gazdă
IPSec protejează traficul de date ce călătoreşte între un gateway şi un calculator gazdă dintr-o reţea la distanţăă. VPN nu protejează traficul de date din reţeaua locală deoarece este considerat de încredere.

Gazdă-la-gateway
VPN protejează traficul de date care călătoreşte între un calculator gazdă din reţeaua locală şi un gateway la distanţă. VPN nu protejează traficul de date din reţeaua la distanţăă.

Gazdă-la-gazdă
Capetele conexiunii sunt aceleaşi cu capetele datelor pe ambele sisteme (local şi la distanţă). VPN protejează traficul de date care călătoreşte între un calculator gazdă din reţeaua locală şi un calculator gazdă din reţeaua la distanţă. Acest tip de VPN furnizează protecţie IPSec end-to-end.

Completarea foilor de lucru pentru planificarea VPN-ului

Folosiţi foile de lucru pentru planificarea VPN pentru a culege informaţii detaliate privind planurile de folosire a VPN-ului. Aveţi nevoie de aceste informaţii pentru a vă planifica în mod adecvat strategia VPN. De asemenea, puteţi folosi aceste informaţii pentru a vă configura VPN-ul. Alegeţi foaia de lucru pentru tipul de conexiune pe care doriţi să-l creaţi.

- **Foaia de lucru pentru planificarea conexiunilor dinamice**
  Completaţi această foaie de lucru înainte de a configura o conexiune dinamică.
- **Foaia de lucru pentru planificarea conexiunilor manuale**
  Completaţi această foaie de lucru înainte de a vă configura o conexiune manuală.
- **Consilierul de planificare VPN**
  Sau, dacă preferaţi, folosiţi consilierul pentru planificare interactivă şi pentru îndrumare la configurare. Consilierul de planificare vă pune întrebări despre reţeaua dumneavoastră şi, pe baza răspunsurilor dumneavoastră, vă furnizează sugestii pentru crearea VPN-ului dumneavoastră.

  Notă: Folosiţi consilierul de planificare VPN doar pentru conexiunile dumneavoastră dinamice. Pentru conexiunile dumneavoastră manuale, folosiţi foaia de lucru pentru planificarea conexiunilor manuale.

Dacă veţi crea conexiuni multiple cu proprietăţi similare, poate doriţi să setaţi valorile implicite VPN. Valorile implicite pe care le configuraţi furnizează informaţiile din foile de proprietăţi VPN. Aceasta înseamnă că nu e necesar să configuraţi aceleaşi proprietăţi de mai multe ori. Pentru a seta valorile implicite VPN, selectaţi **Editare** din meniul principal VPN, şi apoi selectaţi **Defaults**.

Foaia de lucru pentru planificarea conexiunilor dinamice

Înainte de a vă crea conexiunile VPN dinamice, completaţi această foaie de lucru. Foaia de lucru presupune că veţi folosi vrăjitorul de Conexiune nouă. Vrăjitorul vă permite să setaţi un VPN pe baza cerinţelor dumneavoastră primare

de securitate. În anumite cazuri, poate fi nevoie să rafinaţi proprietăţile pe care vrăjitorul le configurează pentru o conexiune. De exemplu, puteţi decide dacă doriţi jurnalizare sau dacă doriţi ca serverul VPN să pornească de fiecare dată când porneşte TCP/IP. În acest caz, faceţi clic dreapta pe grupul sau conexiunea de grup dinamic creată de vrăjitor şi selectaţi **Properties**.

Răspundeţi la fiecare întrebare înainte de a continua cu setarea VPN.

Listă de verificare pentru cerinţele preliminare	**Răspunsuri**
Sistemul dumneavoastră de operare este OS/400(R) V5R2 (5722-SS1) sau ulterior?	
Este instalată opţiunea Digital Certificate Manager (5722-SS1 Option 34)?	
Este instalat Cryptographic Access Provider (5722-AC2 sau AC3)?	
Este instalat iSeries(TM) Access(5722-XE1)?	
Este instalat Navigator iSeries?	
Este instalată subcomponenta de reţea a Navigator iSeries?	
Este instalat TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	
Este configurat TCP/IP în iSeries (inclusiv interfeţele IP, rutele, numele gazdă local, şi numele de domeniu local)?	
Este stabilită comunicaţia TCP/IP normală între punctele cerute?	
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrare pachet IP, regulile filtru ale firewall-ului sau ruterelor suportă protocoalele AH şi ESP?	
Sunt configurate firewall-urile sau ruterele pent ru a permite protocoalele IKE (UDP port 500), AH şi ESP?	
Sunt configurate firewall-urile pentru a permite înaintarea IP?	

Aveţi nevoie de aceste informaţii pentru a configura o conexiune dinamică VPN	**Răspunsuri**
Ce tip de conexiune creaţi? • Gateway-la-gateway • Gazdă-la-gateway • Gateway-la-gazdă • Gazdă-la-gazdă	
Cum veţi denumi grupul de chei dinamice?	
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile? • Cea mai bună securitate, cele mai mici performanţe • Echilibrarea securităţii cu performanţa • Cea mai joasă securitate şi cea mai bună performanţă	
Folosiţi certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată?	
Care este identificatorul serverului local de chei?	
Care este identificatorul punctului final local de date?	
Care este identificatorul serverului de chei la distanţă?	
Care este identificatorul punctului final depărtat de date?	

Aveţi nevoie de aceste informaţii pentru a configura o conexiune dinamică VPN	Răspunsuri
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile? • Cea mai bună securitate, cele mai mici performanţe • Echilibrarea securităţii cu performanţa • Cea mai joasă securitate şi cea mai bună performanţă	

Foaia de lucru pentru planificarea conexiunilor

Completaţi acest tabel pentru a vă ajuta la crearea conexiunilor reţelei dumneavoastră private (VPN) care nu folosesc IKE pentru gestiune cheilor.

Răspundeţi la fiecare din aceste întrebări înainte de a continua cu setarea VPN:

Cerinţe preliminare	Răspunsuri
Sistemul dumneavoastră de operare este OS/400(R) V5R2 (5722-SS1) sau ulterior?	
Este instalată opţiunea Digital Certificate Manager (5722-SS1 Option 34)?	
Este instalat Cryptographic Access Provider (5722-AC2 sau AC3)?	
Este instalat iSeries(TM) Access(5722-XE1)?	
Este instalat Navigator iSeries?	
Este instalată subcomponenta de reţea a Navigator iSeries?	
Este instalat TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	
Este configurat TCP/IP în iSeries (inclusiv interfeţele IP, rutele, numele gazdă local, şi numele de domeniu local)?	
Este stabilită comunicaţia TCP/IP normală între punctele cerute?	
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrare pachet IP, regulile filtru ale firewall-ului sau ruterelor suportă protocoalele AH şi ESP?	
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele AH şi ESP?	
Sunt configurate firewall-urile pentru a permite înaintarea IP?	

Aveţi nevoie de aceste informaţii pentru a configura manual un VPN.	Răspunsuri
Ce tip de conexiune creaţi? • Gazdă-la-gazdă • Gazdă-la-gateway • Gateway-la-gazdă • Gateway-la-gateway	
Cum veţi denumi conexiunea?	
Care este identificatorul capătului local al conexiunii?	
Care este identificatorul capătului la distanţă al conexiunii?	
Care este identificatorul punctului final local de date?	
Care este identificatorul punctului final depărtat de date?	
Ce tip de trafic veţi permite pentru această conexiune (port local, port la distanţă şi protocol)?	
Aveţi nevoie de translatare de adrese pentru această conexiune? Consultaţi Translatarea adreselor de reţea pentru VPN pentru informaţii suplimentare.	

Aveţi nevoie de aceste informaţii pentru a configura manual un VPN.	Răspunsuri
Veţi folosi modul tunel sau modul transport?	
Ce protocol IPSec va folosi conexiunea (AH, ESP sau AH cu ESP)? Consultaţi Securitate IP (IPSec) pentru informaţii suplimentare.	
Ce algoritm de autentificare va folosi conexiune (HMAC-MD5 sau HMAC-SHA)?	
Ce algoritm de criptare va folosi conexiunea (DES-CBC sau 3DES-CBC)? **Notă:** Specificaţi un algoritm de criptare numai dacă aţi selectat ESP ca protocol IPSec.	
Care este cheia de intrare AH? Dacă folosiţi MD5, cheia este un şir hexazecimal de 16 octeţi. Dacă folosiţi SHA, cheia este un şir hexazecimal de 20 de octeţi. Cheia dumneavoastră de intrare trebuie să corespundă exact cheii de ieşire a serverului de la distanţă.	
Care este cheia de ieşire AH? Dacă folosiţi MD5, cheia este un şir hexazecimal de 16 octeţi. Dacă folosiţi SHA, cheia este un şir hexazecimal de 20 de octeţi. Cheia dumneavoastră de ieşire trebuie să corespundă exact cheii de intrarea serverului de la distanţă.	
Care este cheia de intrare ESP? Dacă folosiţi DES, cheia este un şir hexazecimal de 8 octeţi. Dacă folosiţi 3DES, cheia este un şir hexazecimal de 24 de octeţi. Cheia dumneavoastră de intrare trebuie să corespundă exact cheii de ieşire a serverului de la distanţă.	
Care este cheia de ieşire ESP? Dacă folosiţi DES, cheia este un şir hexazecimal de 8 octeţi. Dacă folosiţi 3DES, cheia este un şir hexazecimal de 24 de octeţi. Cheia dumneavoastră de ieşire trebuie să corespundă exact cheii de intrarea serverului de la distanţă.	
Care este Indexul politicii de securitate de intrare (SPI)? SPI de intrare este un şir hexazecimal de 4 octeţi, unde primul octet este setat la 00. SPI-ul dumneavoastră de intrare trebuie să corespundă exact cu SPI-ul de ieşire al serverului de la distanţă.	
Care este SPI-ul de ieşire? SPI de ieşire este un şir hexazecimal de 4 octeţi. SPI-ul dumneavoastră de ieşire trebuie să corespundă exact cu SPI-ul de intrare al serverului de la distanţă.	

Configurarea VPN-ului

Interfaţa VPN vă furnizează câteva moduri diferite de configurare a conexiunilor dumneavoastră VPN. Continuaţi să citiţi pentru a vă putea decide ce tip de conexiune vreţi să configuraţi şi cum să o faceţi.

Ce tip de conexiune ar trebui să configurez?
O conexiune **dinamică** este una care generează şi negociază în mod dinamic cheile care securizează conexiunea, în timp ce este activă, folosind protocolul IKE. Conexiunile dinamice furnizează un nivel în plus de securitate pentru datele care o traversează din cauza schimbării cheilor, automat, la intervale regulate. În consecinţă, este puţin probabil că un atacator poate să captureze o cheie, să aibă timp să o spargă, şi să o folosească la dirijarea sau capturarea traficului pe care cheia îl protejează.

O conexiune **manuală (pagină 36)**, totuşi, nu furnizează suport pentru negocierile IKE şi în consecinţă pentru gestiunea automată a cheilor. Mai departe, amândouă terminările de conexiune necesită să le configuraţi diferite atribute care trebuie să se potrivească exact. Conexiunile manuale folosesc chei statice care nu se reîmprospătează sau schimbă atâta timp cât conexiunea este activă. Trebuie să opriţi o conexiune manuală pentru a schimba cheile sale asociate. În cazul în care consideraţi aceasta un risc de securitate, puteţi vrea să creaţi o conexiune dinamică în schimb.

Cum configurez o conexiune dinamică VPN ?
VPN este de fapt un grup de obiecte de configurare care definesc caracteristicile unei conexiuni. O conexiune dinamică VPN necesită fiecare din aceste obiecte să funcţioneze corect. Urmaţi link-urile de mai jos pentru informaţii specifice despre cum să configurezi fiecare dintre obiectele de configurare VPN:

> **Sugestie:**
> **Configurarea conexiunii cu vrăjitorul Conexiune nou**
> În general, puteţi utiliza vrăjitorul Conexiune pentru a crea toate conexiunile dumneavoastră dinamice. Vrăjitorul creează automat fiecare obiect de configuraţie de care VPN are nevoie pentru a funcţiona corespunzător, inclusiv regulile de pachete. Dacă specificaţi că vreţi ca vrăjitorul să activeze regulile de pachete VPN pentru dumneavoastră, puteţi trece peste pasul 6 de mai jos, *Pornirea conexiunii*. Altfel, după ce vrăjitorul termină configurarea VPN-ului, trebuie să activaţi regulile de pachete şi apoi puteţi porni conexiunea.

Dacă alegeţi să nu folosiţi vrăjitorul pentru a configura conexiunile VPN dinamice, urmaţi aceşti paşi pentru a completa configuraţia:

1. **Configurarea de politici de securitate VPN**
   Trebuie să definiţi politicile de securitate VPN pentru toate conexiunile dumneavoastră dinamice. Politica Internet Key Exchange şi politica de date dictează cum IKE îşi protejează negocierilor de faza 1 şi faza 2.
2. **Configurarea conexiunilor securizate**
   După ce aţi definit politicile de securitate pentru o conexiune, trebuie să configuraţi conexiunea securizată. Pentru conexiunile dinamice, obiectul de conexiune securizată include un grup de chei dinamice şi o conexiune de chei dinamice. **Grupul de chei dinamice** defineşte caracteristicile comune ale uneia sau mai multe conexiuni VPN , în timp ce **conexiunea de chei dinamice** defineşte caracteristicile conexiunilor de date individuale între perechi de puncte finale. Conexiunea de chei dinamice există în grupul de chei dinamice.

   Notă: Puteţi completa doar următorii doi paşi, *Configurarea de reguli pachete* şi *Definirea unei interfeţe pentru reguli*, dacă selectaţi opţiunea **Regula de filtru politici va fi definită în regulile pachete** de la pagina **Grup de chei dinamice - Conexiuni** din interfaţa VPN. Altfel, aceste reguli sunt create ca parte din configuraţiile dumneavoastră VPN şi sunt aplicate la interfaţa pe care o specificaţi.

   Este recomandat să permiteţi întotdeauna ca interfaţa VPN să vă creeze regulile de filtrare a politicii. Faceţi aceasta selectând opţiunea **Generare filtru următor de politică pentru acest grup** în pagina **Grup de chei dinamice - Conexiuni**.
3. **Configurarea de reguli pachete**
   Dupăce completaţi configuraţiile VPN, trebuie să creaţi şi să aplicaţi reguli de filtrare care permit traficului de date să traverseze conexiunea. Regulile VPN **pre-IPSec** permit întregului trafic IKE pe interfeţele specificate astfel încât IKE poate negocia conexiuni. Regula **filtru de politică** defineşte care adrese, protocoale şi porturi pot folosi grupul nou de chei dinamice asociat.

   Dacă migraţi de la V4R4 sau V4R5 şi aveţi conexiuni VPN şi filtre de politică pe care vreţi să continuaţi să le utilizaţi în ediţia curentă, revedeţi subiectul, *Migrare filtre de politică în ediţia curentă* pentru a vă asigura că filtrele de politică vechi şi cele noi vor lucra împreună aşa cum intenţionaţi dumneavoastră.
4. **Definirea unei interfeţe pentru reguli**
   După ce aţi configurat regulile de pachete şi orice altă regulă care aveţi nevoie să activeze conexiunea dumneavoastră VPN, ar trebui să definiţi o interfaţă pe care să le aplicaţi.
5. **Activarea de reguli pachete**
   După ce aţi definit o interfaţă pentru regulile dumneavoastră de pachete, trebuie să le activaţi înainte să puteţi porni conexiunea.
6. **Pornirea conexiunii**
   Finalizaţi această operaţie pentru a porni conexiunile.

Cum configurez o conexiune VPN manuală ?
După cum sugerează şi numele, o conexiune manuală este una unde trebuie să configuraţi toate proprietăţile dumneavoastră VPN manual, inclusiv cheile de intrare şi ieşire. Urmaţi legăturile de mai jos pentru informaţii specifice despre cum să configuraţi o conexiune manuală:

1. **Configurarea de conexiuni manuale**
   Conexiunile manuale definesc caracteristicile unei conexiuni inclusiv tipul de protocoale de securitate conexiunea şi punctele finale de date.

   Notă: Puteţi să completaţi doar următorii doi paşi, *Configurarea regulii de filtrare politici* şi *Definirea unei interfeţe pentru reguli*, dacă selectaţi opţiunea **Regula de filtrare politici va fi definită în regulile de pachete** de la pagina **Conexiune manuală - Conexiune** în interfaţa VPN. Altfel, aceste reguli sunt create ca parte din configuraţiile dumneavoastră VPN.

   Este recomandat să permiteţi întotdeauna ca interfaţa VPN să vă creeze regulile de filtrare a politicii. Faceţi aceasta selectând opţiunea **Generare filtru de politică potrivit cu punctele finale de date**, în pagina **Conexiune manuală - Conexiune**.
2. **Configurarea regulii de filtrare politici**
   După ce configuraţi atributele conexiunii manuale, trebuie să creaţi şi să aplicaţi o regulă de filtrare politici care să permită traficului de date să traveseze conexiunea. Regula de **filtrare politici** defineşte care adrese, protocoale şi porturi pot folosi conexiunea asociată.
3. **Definirea unei interfeţe pentru reguli**
   După ce aţi configurat regulile de pachete şi orice altă regulă care aveţi nevoie să activeze conexiunea dumneavoastră VPN, ar trebui să definiţi o interfaţă pe care să le aplicaţi.
4. **Activarea de reguli pachete**
   După ce aţi definit o interfaţă pentru regulile dumneavoastră de pachete, trebuie să le activaţi înainte să puteţi porni conexiunea.
5. **Pornirea conexiunii**
   Finalizaţi această operaţie pentru a porni conexiunile care sunt iniţiate local.

Configurarea conexiunilor VPN cu vrăjitorul Conexiune nouă

Vrăjitorul de conexiune nouă vă permite să creaţi o reţea privată virtuală (VPN) între orice combinaţie de gazdă şi gateway. De exemplu, gazdă-la-gazdă, gateway-la-gazdă, gazdă-la-gateway sau gateway-la-gateway.

Vrăjitorul creează automat fiecare obiect de configuraţie de care VPN are nevoie pentru a funcţiona corespunzător, inclusiv regulile de pachete. Totuşi, dacă aveţi nevoie să adăugaţi funcţii la VPN, de exemplu jurnalizare sau translatarea adreselor de reţea pentru VPN (VPN NAT), aţi putea să vă rafinaţi VPN prin tabelele de proprietăţi ale grupurilor de chei dinamice sau conexiunilor corespunzătoare. Pentru aceasta, trebuie să opriţi întâi conexiunea dacă este activă. Apoi faceţi clic dreapta pe grupul de chei dinamice sau conexiune şi selectaţi **Proprietăţi**.

Completaţi Consilierul de planificare VPN înainte de a începe. Consilierul vă furnizează un mijloc de a aduna informaţii importante de care aveţi nevoie pentru a crea VPN.

Pentru a crea un VPN cu vrăjitorul de conexiune, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi**Conexiune nouă** pentru a porni vrăjitorul.
3. Finalizaţi vrăjitorul pentru a crea o conexiune VPN de bază. Faceţi clic pe **Ajutor**, dacă aveţi nevoie de ajutor.

Configuraţi politicile de securitate VPN

După ce determinaţi cum veţi folosi VPN-ul, trebuie să vă definiţi politicile de securitate pentru VPN. Mai precis, va trebui să:

- **Configuraţi o politică Internet Key Exchange (IKE)**
  Politica IKE defineşte ce nivel de autentificare şi protecţie prin criptare foloseşte IKE în timpul fazei 1 a negocierilor. Faza 1 IKE stabileşte cheile care protejează mesajele care se transmit în negocierile următoare din faza 2. Nu este nevoie să definiţi o politică IKE când creaţi o conexiune manuală. În plus, dacă vă creaţi VPN-ul cu vrăjitorul Conexiune nouă, acesta poate crea politica IKE în locul dumneavoastră.
- **Configuraţi o politică de date**
  O politică de date defineşte ce nivel de autentificare sau criptare protejează datele care circulă prin VPN. Sistemele care comunică cad de acord asupra acestor atribute în timpul negocierilor din faza 2 a protocolului Internet Key

Exchange (IKE). Nu este nevoie să definiţi o politică de date când creaţi o conexiune manuală. În plus, dacă vă creaţi VPN-ul cu vrăjitorul Conexiune nouă, acesta poate crea politica de date în locul dumneavoastră.

După ce configuraţi politicile de securitate VPN, trebuie apoi să configuraţi conexiunile securizate.

Configurarea unei politici IKE (Internet Key Exchange)

O politică IKE defineşte ce nivel de autentificare sau protecţie prin criptare foloseşte IKE în timpul negocierilor din faza 1. Faza 1 IKE stabileşte cheile care protejează mesajele care se transmit în negocierile următoare din faza 2. VPN foloseşte fie modul semnătură RSA, fie chei prepartajate pentru a autentifica negocierile de fază 1. Dacă aveţi de gând să folosiţi certificate digitale pentru autentificarea serverelor de chei, trebuie întâi să le configuraţi folosind Digital Certificate Manager (5722-SS1 Opţiunea 34). Politica IKE de asemenea identifică ce server de chei la distanţă va folosi această politică.

Pentru a defini o politică IKE sau pentru a face modificări la una existentă, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP -> Reţea privată virtuală—> Politici securitate IP**.
2. Pentru a crea o nouă politică, faceţi clic dreapta pe **Politici Internet Key Exchange** şi selectaţi **Politică nouă Internet Key Exchange**. Pentru a face modificări la o politică existentă, apăsaţi pe **Politici Internet Key Exchange** în panoul stâng, apoi faceţi clic dreapta pe politica de date pe care vreţi să o modificaţi în panoul drept şi selectaţi **Proprietăţi**.
3. Completaţi fiecare tabel de proprietăţi. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Notă: Se recomandă să folosiţi negocierea mod principal de fiecare dată când este folosită o cheie prepartajată pentru autentificare. În acest fel, schimbul este mai sigur. Dacă trebuie să utilizaţi chei prepartajate şi negocierea mod agresiv, selectaţi parole pentru care este puţin probabil să fie sparte în atacurile care scanează dicţionarul. Se recomandă de asemenea să vă modificaţi periodic parolele. Utilizaţi ajutorul online al Navigatorului iSeries pentru detalii suplimentare.

Configurarea unei politici de date

O politică de date defineşte ce nivel de autentificare sau criptare protejează datele care circulă prin VPN. Sistemele care comunică cad de acord asupra acestor atribute în timpul negocierilor din faza 2 ale protocolului Internet Key Exchange (IKE).

Pentru a defini o politică de date sau pentru a face modificări la una existentă, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP -> Reţea privată virtuală—> Politici securitate IP**.
2. Pentru a crea o nouă politică de date, faceţi clic dreapta pe **Politici de date** şi selectaţi **Politică de date nouă**. Pentru a face modificări la o politică de date existentă, apăsaţi pe **Politici de date** (în panoul stâng) apoi faceţi clic dreapta pe politica de date pe care vreţi să o modificaţi (în panoul drept) şi selectaţi **Proprietăţi**.
3. Completaţi fiecare tabel de proprietăţi. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Configurarea conexiunilor sigure VPN

După ce aţi configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configuraţi conexiunea sigură. Pentru conexiunile dinamice, obiectul de conexiune securizată include un grup de chei dinamice şi o conexiune de chei dinamice.

Grupul chei dinamice defineşte caracteristicile comune ale uneia sau mai multe conexiuni VPN. Configurarea unui grup de chei dinamice vă permite să folosiţi aceleaşi politici, dar puncte finale de date diferite pentru fiecare conexiune din grup. Grupurile de chei dinamice de asemenea vă permit să negociaţi cu succes cu iniţiatori de la distanţă când punctele finale propuse de sistemul de la distanţă nu sunt cunoscute în mod special dinainte. Aceasta se face prin asocierea informaţiilor despre politici din grupul de chei dinamice cu o regulă de filtrare politici cu un tip acţiune IPSEC. Dacă punctele finale de date specifice oferite de iniţiatorul de la distanţă sunt în intervalul specificat în regula de filtrare IPSEC, ele pot fi subiectul politicii definite în grupul de chei dinamice.

Conexiunea chei dinamice defineşte caracteristicile conexiunilor individuale de date dintre perechi de puncte finale. Conexiunea de chei dinamice există în grupul de chei dinamice. După ce configuraţi un grup cheie dinamică pentru a descrie ce politici utilizează conexiunile din grup, trebuie să creaţi conexiuni cheie dinamică individuale pentru cele pe care le iniţiaţi local.

Pentru a configura obiectul conexiune sigură, executaţi aceste operaţii:

Partea 1: Configuraţi un grup de chei dinamice:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**.
2. Apăsaţi pe **După grup** şi selectaţi **Grup nou de chei dinamice**.
3. Apăsaţi pe **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Partea 2: Configuraţi o conexiune chei dinamice:

1. În Navigator iSeries, expandaţi **—> Reţea —> Politici IP —> Reţea privată virtuală —> Conexiuni sigure —> după grup**.
2. În panoul din stânga al ferestrei Navigatorului iSeries, faceţi clic dreapta pe grupul de chei dinamice pe care l-aţi creat în partea întâi şi selectaţi **Conexiune nouă de chei dinamice**.
3. Apăsaţi pe **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

După ce aţi făcut aceşti paşi, trebuie să activaţi regulile pachet pe care le cere conexiunea pentru a funcţiona corespunzător.

Notă: În mojoritatea cazurilor, permiteţi interfeţei VPN să genereze reguli pachet VPN automat prin selectarea opţiunii **Generare următoarul filtru politică pentru acest grup** în pagina **Grup cheie dinamică - conexiuni**. Însă dacă selectaţi opţiunea **Filtrul de politici va fi definit în Reguli pachet**, atunci trebuie să configuraţi reguli de filtrare VPN folosind editorul Reguli pachet şi apoi să le activaţi.

Configurarea unei conexiuni manuale

Aşa cum sugerează numele, o conexiune manuală este una în care trebuie să configuraţi toate proprietăţile VPN de mână. Mai mult, ambele capete ale conexiunii vă cer să configuraţi câteva elemente care trebui să se potrivească *exact*. De exemplu, cheile dumneavoastră de intrare trebuie să se potrivească cu cheile de ieşire ale sistemuului de la distanţă, altfel conexiunea va eşua.

Conexiunile manuale folosesc chei statice care nu sunt reîmprospătate sau schimbate cât timp conexiunea este activă. Trebuie să opriţi o conexiune manuală pentru ai schimba cheie asociată. Dacă credeţi că acesta este un risc de securitate şi ambele capete ale conexiunii suportă protocolul IKE, aţi putea folosi o conexiune dinamcă.

Pentru a defini proprietăţile conexiunii dumneavoastră manuale, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**.
2. Faceţi clic dreapta pe **Toate conexiunile** şi selectaţi **Conexiune manuală nouă**.

3. Completaţi fiecare tabel de proprietăţi. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Notă: În mojoritatea cazurilor, permiteţi interfeţei VPN să genereze reguli pachet VPN automat prin selectarea opţiunii **Generare filtru politică care se potriveşte cu punctele finale de date** în pagina **Conexiune manuală - conexiune**. Totuşi, dacă selectaţi opţiunea **Filtrul de politică va fi definit în Reguli pachet** , atunci trebuie să configuraţi o regulă de filtrare a politicii de mână şi apoi să o activaţi.

Configurarea regulilor de pachete VPN

Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Dacă decideţi să creaţi regulile pachet VPN utilizând editorul Reguli pachet din Navigator iSeries(TM), creaţi şi alte reguli suplimentare în acelaşi fel. Invers, dacă lăsaţi VPN-ul să vă genereze regulile filtru politică, creaţi toate regulile filtru politică suplimentare în acest mod.

În general, VPN cere două tipuri de reguli de filtrare: reguli de filtrare Pre-IPSec şi reguli de filtrare de politici. Revedeţi subiectele de mai jos pentru a afla cum se configurează aceste reguli folosind editorul de reguli de pachete din Navigator iSeries. Dacă vreţi să citiţi despre alte opţiuni VPN şi de filtrare, vedeţi secţiunea *Filtrare VPN şi IP* din subiectul concepte VPN.

- **Reguli pre-IPSec**
  Regulile pre-IPSec sunt orice reguli care din sistem care vin înainte de regulile cu un tip de acţiune IPSEC. Acest subiect discută doar despre regulile pre-IPSec cerute de VPN pentru a funcţiona corespunzător. În acest cay, regulile pre-IPSec sunt o pereche de reguli care permit procesarea IKE peste conexiune. IKE permite ca generarea şi negocierea dinamică de chei să aibe loc pe conexiunea dumneavoastră. Aţi putea avea nevoie să adăugaţi alte reguli pre-IPSec, depinzând de mediul particular de reţea şi de politica de securitate.

  Notă: Trebuie să configuraţi acest tip de regulă pre-IPSec ddoar dacă aveţi deja alte reguli care permit IKE pentru sisteme specifice. Dacă nu există reguli de filtrare special pentru permiterea traficului IKE, atunci acesta este implicit permis.
- **Regula de filtrare politică**
  Regula de filtrare politică defineşte traficul care poate folosi VPN şi ce politică de protecţie a datelor să se aplice acestui trafic.

Lucruri de luat în seamă înainte de a începe
Când adăugaţi reguli de filtrare pentru a interfaţă, sistemul adaugă automat o regulă implicită de negare pentru acea interfaţă. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteţi şi nu puteţi schimba această regulă. Ca rezultat, puteţi vedea că trafic care înainte trecea, în mod misterios nu mai funcţionează după ce activaţi regulile de filtrare VPN. Dacă doriţi să permiteţi alt trafic decât VPN prin interfaţă, trebuie să adăugaţi reguli explicite de permitere.

După ce configuraţi regulile de filtrare corespunzătoare, trebuie să definiţi interfaţa la care ele se aplică, apoi să le activaţi.

Este esenţial să vă configuraţi regulile de filtrare corespunzător. Altfel, regulile de filtrare pot bloca tot traficul IP care vine şi vine şi pleacă din iSeries. Aceata include şi conexiunea cu Navigator iSeries, pe care o folosiţi pentru a configura regulile de filtrare.

Dacă regulile de filtrare nu permit traficul pentru Navigator iSeries, Navigator iSeries nu poate să comunice cu iSeries. Dacă vă găsiţi în această situaţie, trebuie să vă logaţi pe serverul dumneavoastră iSeries utilizând o interfaţă care are încă conectivitate, cum ar fi consola de operaţii. Folosiţi comanda RMVTCPTBL pentru a înlătura toate filtrele din sistem. Această comandă de asemenea opreşte toate serverele *VPN apoi le porneşte din nou. Apoi configuraţi filtrele şi reactivaţi-le.

Configurarea regulii de filtrare pre-IPSec

Atenţie: Efectuaţi această operaţie doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile filtrare politică automat.

O pereche de servere IKE (Internet Key Exchange) negociază dinamic şi reîmprospătează cheile. IKE foloseşte bine-cunoscutul port, 500. Pentru ca IKE să funcţioneze corespunzător, trebuie să permiteţi datagramele UDP pe portul 500 pentru acest trafic IP. Pentru a face aceasta, veţi crea o pereche de reguli de filtrare; una pentru traficul de intrare şi una pentru traficul de ieşire, astfel încât conexiunea dumneavoastră să poată negocia dinamic cheile pentru a proteja conexiunea:

1. În Navigator iSeries(TM), expandaţi-vă serverul —> **Reţea**—> **Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru iSeries-ul dumneavoastră.
3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare —> Filtru**.
5. În pagina **General**, specificaţi un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puţin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică şi unul pentru regulile de filtru PERMITERE şi REFUZARE. Numiţi setul care conţine regulile dumneavoastră de filtru pre-IPSec cu prefixul *preipsec*. De exemplu, preipsecfilters.
6. În câmpul **Acţiune**, selectaţi **PERMITERE** din lista derulantă.
7. În câmpul **Direcţie**, selectaţi **DE IEŞIRE** din lista derulantă.
8. În câmpul **Nume adresă sursă**, selectaţi **=** din prima listă derulantă şi apoi introduceţi adresa IP a serverului local de chei în al doilea câmp. Aţi specificat adresa IP a serverului local de chei în politica IKE.
9. În câmpul **Nume adresă destinaţie**, selectaţi **=** din prima listă derulantă şi apoi introduceţi adresa IP a serverului la distanţă de chei în al doilea câmp. Aţi specificat de asemenea adresa IP a serverului la distanţă de chei în politica IKE.
10. În pagina **Servicii**, selectaţi **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**.
11. În câmpul **Protocol**, selectaţi **UDP** din lista derulantă.
12. Pentru **Portul sursă**, selectaţi **=** în primul câmp, apoi introduceţi 500 în al doilea câmp.
13. Repetaţi pasul anterior pentru **Portul destinaţie**.
14. Apăsaţi **OK**.
15. Repetaţi aceşti paşi pentru a configura filtrul INBOUND. Folosiţi acelaşi nume de set şi inversaţi adresele dacă e nevoie.

Notă: O opţiune mai puţin sigură, dar mai uşoară pentru permiterea traficului IKE prin conexiune, este să configuraţi doar un filtru pre-IPSec şi să folosiţi valori joker (*) în câmpurile **Direcţie**, **Nume adresă sursă** şi **Nume adresă destinaţie**.

Următorul pas este să configuraţi o regulă de filtrare politici pentru a defini ce trafic IP protejează conxiunea VPN.

Configurarea unei reguli filtrare politici

Atenţie: Efectuaţi această operaţie doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile filtrare politică automat.

Regula de filtrare politici (o regulă în care action=IPSEC) defineşte care adrese, protocoale şi porturi pot folosi VPN-ul. De asemenea, identifică politica aplicată traficului din conexiunea VPN. Pentru a configura o regulă de filtrare politici, parcurgeţi paşii următori:

Notă: Dacă doar aţi ocnfigurat regula pre-IPSec (doar pentru conexiuni dinamice) editorul Reguli pachetva fi încă deschis; deplsaţi-vă la pasul patru.

1. În Navigator iSeries(TM), expandaţi-vă serverul —> **Reţea**—> **Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru iSeries-ul dumneavoastră.

3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare —> Filtru**.
5. În pagina **General**, specificaţi un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puţin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică şi unul pentru regulile de filtru PERMITERE şi REFUZARE. De exemplu, policyfilters
6. În câmpul **Acţiune**, selectaţi **IPSEC** din lista derulantă. Câmpul **Direcţie** este implicit pe DE IEŞIRE şi nu puteţi să-l schimbaţi. Deşi acest câmp este implicit pe OUTBOUND, este de fapt bi-direcţional. Apare OUTBOUND pentru a clarifica semantica valorilor de intrare. De exemplu, valorile sursă sunt valori locale şi valorile destinaţie sunt valori la distanţă.
7. Pentru **Nume adresă sursă**, selectaţi **=** în primul câmp şi apoi introduceţi adresa IP a punctului final local de date în al doilea câmp. Puteţi de asemenea să specificaţi un interval de adrese IP sau o adresă IP plus o mască de subreţea după ce le definiţi folosind funcţia **Definire Adrese**.
8. Pentru **Nume adresă destinaţie**, selectaţi **=** în primul câmp şi apoi introduceţi adresa IP a punctului final la distanţă de date în al doilea câmp. Puteţi de asemenea să specificaţi un interval de adrese IP sau o adresă IP plus o mască de subreţea după ce le definiţi folosind funcţia **Definire Adrese**.
9. În câmpul **Jurnalizare**, specificaţi ce nivel de jurnalizare aveţi nevoie.
10. În câmpul **Nume conexiune**, selectaţi definiţia conexiunii la care se aplică aceste reguli de filtrare.
11. (opţional) Introduceţi o descriere.
12. În pagina **Servicii**, selectaţi **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**.
13. În câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**, selectaţi valoarea corespunzătoare pentru trafic. Sau, puteţi selecta asteriscul (*) din lista derulantă. Aceasta permite oricărui protocol care foloseşte orice port să folosească VPN.
14. Apăsaţi **OK**.

Următorul pas este să definiţi interfaţa la care se aplică aceste reguli de filtrare.

Notă: Când adăugaţi reguli de filtrare pentru o interfaţă, sistemul adaugă automat o regulă implicită REFUZARE pentru acea interfaţă. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteţi şi nu puteţi schimba această regulă. În consecinţă, s-ar putea să vedeţi că anumite conexiuni care au funcţionat anterior eşuează misterios după ce vă activaţi regulile pachet VPN. Dacă doriţi să permiteţi alt trafic decât VPN prin interfaţă, trebuie să adăugaţi reguli explicite de permitere.

Definirea interfeţei pentru regulile de filtru VPN

După ce v-aţi configurat regulile pachet VPN şi orice alte reguli de care aveţi nevoie, pentru a vă activa conexiunea VPN trebuie să definiţi interfaţa la care se aplică.

Pentru a defini o interfaţă la care să vă aplicaţi regulile de filtrare VPN, parcurgeţi paşii următori:

Notă: Dacă doar aţi configurat regulile pachet VPN, interfaţa Reguli pachet va fi încă deschisă; deplasaţi-vă la pasul patru.

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru iSeries-ul dumneavoastră.
3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare —> Filtru interfaţă**.
5. În pagina **General**, selectaţi **Nume linie** şi apoi selectaţi din lista derulantă descrierea liniei la care se aplică regulile pachet VPN.
6. (opţional) Introduceţi o descriere.
7. În pagina **Seturi filtre**, apăsaţi **Adăugare** pentru a adăuga fiecare nume de set pentru filtrele pe care tocmai le-aţi configurat.
8. Apăsaţi **OK**.

9. Salvaţi fişierul cu regulile dumneavoastră. Fişierul este salvat în sistemul de fişiere integrat de pe sistemul dumneavoastră iSeries cu extensia .i3p.
   Notă: Nu vă salvaţi fişierul în următorul director:

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

   Acest director este doar folosit doar de sistem. Dacă aveţi nevoie să folosiţi comanda RMVTCPTBL *ALL să dezactivaţi regulile pachet, comanda va şterge toate fişierele din acest director.

După ce definiţi o interfaţă pentru regulile dumneavoastră de filtrare, trebuie să le activaţi înainte de a putea porni VPN.

Activarea regulilor pachet VPN

Trebuie să activaţi regulile pachet VPN înainte de a vă putea porni conexiunile VPN. Nu puteţi activa (sau deactiva) regulile pachet când aveţi conexiuni VPN care rulează pe sistemul dumneavoastră. Aşa că, înainte să vă activaţi regulile de filtrare VPN, asiguraţi-vă că nu există conexiuni active asociate cu ele.

Dacă v-aţi creat conexiunile VPN cu vrăjitorul Conexiune nouă, puteţi alege să aveţi activate regulile asociate, automat, pentru dumneavoastră. Ţineţi cont că, dacă sunt active alte reguli pachet pe oricare din interfeţele pe care le specificaţi, regulile de filtrare ale politicii VPN le vor înlocui.

Dacă alegeţi să vă activaţi regulile generate VPN folosind Editorul reguli pachet, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectaţi dacă vreţi să activaţi doar regulile generate VPN, doar un fişier selectat sau ambele variante. Puteţi alege ultima variantă, de exemplu, dacă aveţi diverse reguli PERMITERE şi REFUZARE pe care doriţi să le impuneţi pe interfaţă în plus faţă de regulile generate VPN.
4. Selectaţi interfaţa pe care vreţi să activaţi regulile. Puteţi alege să activaţi pe o anumită interfaţă, pe un identificator punct-la-punct sau pe toate interfeţele şi toţi identificatorii punct-la-punct.
5. Faceţi clic pe **OK** în caseta de dialog pentru a confirma ca vreţi să verificaţi şi să activaţi regulile pe interfaţa sau interfeţele specificate. După ce aţi apăsat OK, sistemul verifică regulile de erori sintactice şi semantice şi raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fişier anume şi un număr de linie, puteţi apăsa clic dreapta pe eroare şi selecta **Mergi la linie** pentru a evidenţia eroarea în fişier.

După ce vă activaţi regulile de filtrare, vă puteţi porni conexiunea VPN.

Pornirea unei conexiuni VPN

Aceste instrucţiuni pleacă de la premisa că aţi configurat corespunzător conexiunea VPN. Urmaţi aceşti paşi pentru a porni conexiunea VPN:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Dacă serverul VPN nu este pornit, faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Pornire**. Aceasta porneşte serverul VPN.
3. Asiguraţi-vă că regulile dumneavoastră pachet sunt activate.
4. Expandaţi **Reţea privată virtuală —> Conexiuni sigure**.
5. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
6. Faceţi clic dreapta pe conexiunea pe care vreţi să o porniţi şi selectaţi **Pornire**. Pentru a porni mai multe conexiuni, selectaţi fiecare conexiune pe care doriţi să o porniţi, faceţi clic dreapta şi selectaţi **Pornire**.

Administrarea VPN

Utilizaţi interfaţa VPN din Navigator iSeries(TM) pentru a manipula toate trask-urile de gestiune, inclusiv:

- **Pornirea unei conexiuni VPN**
  Finalizaţi această operaţie pentru a porni conexiuni pe care le iniţiaţi local.

- **Setarea de atribute implicite pentru conexiunile dumneavoastră**
  Valorile implicite apar în panourile pe care le folosiţi să creaţi noi politici şi conexiuni. Puteţi seta valori implicite pentru nivelurile de securitate, pentru administrarea sesiunilor de chei, pentru duratele de viaţă ale cheilor şi pentru duratele de viaţă ale conexiunilor.
- **Resetarea conexiunilor dintr-o stare de eroare**
  Refacerea conexiunilor dintr-o eroare le întoarce la starea idle.
- **Vizualizarea de informaţii de eroare**
  Finalizaţi această operaţie pentru a vă ajuta să determinaţi de ce conexiunea dumneavoastră are o eroare.
- **Vizualizarea atributelor conexiunilor active**
  Finalizaţi această operaţie pentru a verifica starea şi alte atribute ale conexiunilor dumneavoastră active.
- **Folosiţi urmărirea serverului VPN**
  Urmărirea serverului VPN vă permite să configuraţi, să porniţi, să opriţi şi să vizualizaţi urmăririle server VPN Connection Manager şi VPN Key Manager. Acesta este similar cu folosirea comenzii TRCTCPAPP *VPN din interfaţa bazată pe caractere cu excepţia că puteţi vedea urmărirea cât timp o conexiune este activă.
- **Vizualizarea fişierelor jurnal job ale serverului VPN**
  Urmaţi aceste instrucţiuni pentru a vedea fişierele jurnal de joburi din VPN Key Manager şi VPN Connection Manager.
- **Oprirea conexiunilor**
  Finalizaţi această operaţie pentru a opri conexiuni active.
- **Vizualizarea atributelor Asocierilor de securitate (Security Associations - SA)**
  Finalizaţi această operaţie pentru a afişa atributele Asocierilor de securitate (Security Associations - SAs) care sunt asociate cu o conexiune activată.
- **Ştergerea obiectelor de configurare VPN**
  Înainte să ştergeţi un obiect de configurare VPN din baza de date de politici VPN, asiguraţi-vă că înţelegeţi cum afectează alte conexiuni şi grupuri de conexiuni VPN.

Setarea atributelor implicite pentru conexiunile dumneavoastră

Valorile de securitate implicite au furnizat date către diverse câmpuri când aţi creat iniţial noile obiecte VPN.

Pentru a seta valorile de securitate implicite pentru conexiunile dumneavoastră VPN, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţi clic pe **Reţea privată virtuală** şi selectaţi **Valori implicite**.
3. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** după ce aţi completat fiecare din paginile de proprietăţi.

Resetarea conexiunilor în starea de eroare

Pentru a reîmprospăta o conexiune care este în stare de eroare, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o resetaţi şi selectaţi **Resetare**. Aceasta resetează conexiunea la starea inactiv. Pentru a reseta mai multe conexiuni care sunt în stare de eroare, selectaţi fiecacre conexiune pe care doriţi să o resetaţi, faceţi clic dreapta şi selectaţi **Resetare**.

Vizualizarea informaţiei de eroare

Pentru a vizualiza informaţiile despre conexiunile eronate, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea eronată pe care vreţi să o vedeţi şi selectaţi **Informaţii despre eroare**.

Vizualizarea atributelor conexiunilor active

Pentru a vedea atributele curente ale unei conexiuni active sau la cerere, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea activă sau la cerere pe care doriţi să o vizualizaţi şi selectaţi **Proprietăţi.**
4. Mergeţi la pagina **Atribute curente** pentru a vedea atributele conexiunii.

De asemenea, puteţi vedea atributele tuturor conexiunilor din fereastra Navigator iSeries. În mod implicit, singurele atribute care sunt afişate sunt Stare, Descriere şi Tipul conexiunii. Puteţi schimba ce date vor fi afişate prin următorii paşi:

1. În Navigator iSeries, expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**.
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Din meniul **Obiecte**, selectaţi **Coloane**. Aceasta deschide o casetă de dialog care vă permite să selectaţi care atribute vreţi să le afişaţi în fereastra Navigatorului iSeries.

Fiţi atent că atunci când schimbaţi coloanele de vizualizat, schimbările nu sunt specifice unui anume utilizator sau PC ci, mai degrabă, sunt valabile în întregul sistem.

Folosirea urmăririi serverului VPN (VPN server trace)

Pentru a vizualiza o urmărire de server VPN, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţui clic dreapta pe **Reţea privată virtuală**, selectaţi **Unelte de diagnoză**, şi apoi **Urmărire server**.

Pentru a specifica tipul de urmărire pe care doriţi să-l genereze VPN Key Manager şi VPN Connection Manager, parcurgeţi paşii următori:

1. Din fereastra **Reţea privată virtuală**, apăsaţi

   (Opţiuni).
2. În pagina **Manager conexiuni**, specificaţi ce tip de urmărire doriţi să ruleze serverul Manager conexiuni.
3. În pagina **Manager chei**, specificaţi ce tip de urmărire doriţi să ruleze serverul Manager chei.
4. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
5. Apăsaţi **OK** pentru a salva modificările.
6. Apăsaţi

   (Pornire) pentru a porni urmărirea. Apăsaţi

   (Reîmprospătare) periodic pentru a vedea ultimele informaţii de urmărire.

Vizualizarea fişierelor jurnal job ale serverului VPN

Pentru a vedea fişierele jurnal job curente ale VPN Key Manager sau ale VPN Connection Manager, urmaţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP.**
2. Faceţi clic dreapta pe **Reţea privată virtuală**, selectaţi **Unelte de diagnoză** şi apoi selectaţi istoricul jobului de server pe care doriţi să-l vizualizaţi.

Vizualizarea atributelor Asocierilor de securitate (Security Associations - SA)

Pentru a vedea atributele asocierilor de securitate care sunt asociate cu o conexiune activă. Pentru a face asta, urmaţi paşii de mai jos:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea activă corespunzătoare şi selectaţi **Asocieri de securitate.**Fereastra rezultată vă permite să vizualizaţi proprietăţile fiecărei dintre SA-urile asociate cu o conexiune specifică.

Oprirea unei conexiuni VPN

Pentru a opri o conexiune activă sau la-cerere, parcurgeţi paşii următori:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o opriţi şi selectaţi **Oprire**. Pentru a opri mai multe conexiuni, selectaţi fiecare conexiune pe care doriţi să o opriţi, faceţi clic dreapta şi selectaţi **Oprire**.

Ştergerea obiecteleor de configurare VPN

Dacă sunteţi sigur că aveţi nevoie să ştergeţi o conexiune VPN din baza de date de politici VPN, executaţi următorii paşi:

1. În Navigator iSeries(TM), expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o ştergeţi şi selectaţi **Ştergere**.

Depanarea VPN

VPN este o tehnologie complexă care se schimbă rapid şi care necesită cel puţin cunoştiinţe de bază privind tehnologiile IPSec obişnuite. Trebuie de asemenea să fiţi familiarizat cu regulile pachet IP deoarece VPN necesită câteva reguli filtru pentru a funcţiona corect. Din cauza acestei complexităţi, s-ar putea să experimentaţi, din când în când, probleme cu conexiunile dumneavoastră VPN. Depanarea VPN nu este întotdeauna o sarcină uşoară. Trebuie să vă înţelegeţi mediile de reţea şi de sistem, cât şi componentele pe care le folosiţi când obişnuiţi să le gestionaţi. Următoarele subiecte vă sugerează indicii despre cum să depanaţi problemele diverse pe care le puteţi întâlni când folosiţi VPN:

- **Începeţi depanarea VPN**
  Mergeţi aici pentru a începe găsirea şi corectarea problemelor de conexiune VPN.
- **Erori de configurare VPN comune şi cum să le reparaţi**
  Acest subiect identifică cele mai comune erori ale utilizatorilor şi furnizează soluţii posibile.
- **Depanarea VPN cu jurnalul QIPFILTER**
  Acest subiect furnizează informaţii despre regulile de filtrare VPN.
- **Depanarea VPN cu jurnalul QVPN**
  Acest subiect furnizează informaţii despre traficul IP şi conexiuni.
- **Depanare VPN cu jurnalele de job VPN**
  Acest subiect descrie diversele jurnale de job pe care le foloseşte VPN.
- **Depanare VPN cu Urmărire comunicaţii OS/400(R)**
  Acest subiect descrie cum să urmăriţi date pe o linie de comunicare.

Începeţi depanarea VPN

Există câteva moduri de a începe analizarea problemelor VPN:

1. Asiguraţi-vă întotdeauna că aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?
2. Asiguraţi-vă că îndepliniţi Cerinţele minime pentru setarea VPN.
3. Revedeţi orice mesaj de eroare găsit în fereastra Informaţii de Eroare sau în Jurnalele serverului VPN atât pentru sistemul local , cât şi pentru cel la distanţă. De fapt când depanaţi probleme de conexiuni VPN, este adesea necesar să priviţi ambele capete ale conexiunii. Mai departe, trebuie să luaţi în considerare faptul că trebuie să verificaţi patru adrese: capetele local şi la distanţă ale conexiunii, care sunt adresele unde IPSec este aplicat la pachete, şi punctele finale de date local şi la distanţă, care sunt adrese sursă şi destinaţie ale pachetelor IP.
4. Dacă mesajele de eoare găsite nu aduc suficiente informaţii pentru a rezolva problema, verificaţi jurnalul Filtru IP.
5. Urmărirea comunicaţiei pe iSeries(TM) vă oferă un alt loc în care găsiţi informaţii generale despre faptul că sistemul local primeşte sau trimite cereri de conexiune.
6. Comanda Trace TCP Application (TRCTCPAPP) furnizează o altă cale de a izola probleme. Tipic, serviciul IBM(R) utilizează TRCTCPAPP pentru a obţine ieşire de urmărire pentru a analiza problemele de conexiune.

Alte lucruri de verificat

Dacă apare o eroare după ce setaţi o conexiune şi nu sunteţi sigur unde a apărut eroarea în reţea, incercaţi să reduceţi complexitatea mediului dumneavoastră de lucru. De exemplu, în loc să investigaţi toate părţile unei conexiuni VPN o dată, începeţi cu conexiunea IP. Lista următoare vă dă câteva indicaţii de bază despre cum să porniţi analizarea problemelor VPN, de la cele mai simple conexiuni IP la mai complexele conexiuni VPN:

1. Începeţi cu o configuraţie IP între gazda locală şi cea de la distanţă. Înlăturaţi orice filtre IP din interfaţa folosită de sistemul local şi cel la distanţă pentru comunicaţie. Puteţi face ping de la gazda locală la gazda de la distanţă?

   Notă: Amintiţi-vă să promptaţi pe comanda PING; introduceţi adresa sistemului la distanţă şi folosiţi PPF10 pentru parametri suplimentari, apoi introduceţi adresa IP locală. Aceasta este important mai ales când aveţi mai multe interfeţe fizice şi logice. Asigură că sunt plasate adresele corecte în pachetele PING.

   Dacă răspundeţi **da**, treceţi la pasul 2. Dacă răspundeţi **nu**, verificaţi conficuraţia IP, starea interfeţei şi intrările de rutare. Dacă configurarea este corectă, folosiţi monitorizarea comunicaţiei pentru a verifica de exemplu că cererea IP părăseşte sistemul. Dacă trimiteţi o cerere PING şi nu primiţi răspuns, problema este probabil în reţea sau la sistemul la distanţă.

   Notă: Pot exista rutere sau firewall-uri intermediare care filtrează pachetle IP şi ar putea opri pachetele PING. PING este bazat de obicei pe protocolul ICMP. Dacă PING reuşeşte, ştiţi că există legătura. Dacă PING nu reuşeşte, şitţi doar că a eşuat PING. Aţi putea încerca alte protocoale IP între cele două sisteme, de exemplu Telnet sau FTP, pentru a testa cenexiunea.
2. Verificaţi regulile de filtrare pentru VPN şi asiguraţi-vă că sunt activate. Porneşte filtrarea cu bine? Dacă răpundeţi **da**, treceţi la pasul 3. Dacă răspundeţi **nu**, verificaţi mesajele de eroare din fereastra Reguli pachet din Navigator iSeries. Asiguraţi-vă că regulile de filtrare nu specifică Translatarea Adreselor de Reţea (NAT) pentru traficul VPN.
3. Porniţi conexiunea dumneavoastră VPN . Porneşte conexiunea cu bine? Dacă răspundeţi **da**, mergeţi la pasul 4. Dacă răpundeţi **nu**, verificaţi jurnalul QTOVMAN şi QTOKVPNIKE pentru erori.
   Când folosiţi VPN-ul, furnizorul dumneavoastră de servicii Internet (ISP) şi fiecare gateway de securitate din reţeaua dumneavoastră trebuie să suporte protocoalele Authentication Header (AH) şi Encapsulated Security Payload (ESP). Dacă alegeţi să folosiţi AH sau ESP depinde de propunerile pe care le definiţi pentru conexiunile dumneavoastră VPN.
4. Puteţi activa o sesiune utilizator peste coenxiunea VPN? Dacă răspundeţi **da**, atunci conexiunea VPN funcţionează aşa cum aţi cerut. Dacă răspundeţi **nu**, atunci verificaţi regulile pachet şi grupurile cheie dinamică VPN şi conexiunile pentru definiţiile filtru care nu permit traficul utilizator pe care îl vreţi.

Erori comune de configurare VPN şi cum se pot repara

Această secţiune descrie câteva dintre cele mai obişnuite probleme care apar cu VPN şi vă face legătura cu sugestii şi cum să le rezolvaţi.

Notă: Când configuraţi VPN, creaţi de fapt mai multe obiecte diferite de configurare, fiecare cerut de VPN pentru a activa conexiunea. În termeni de VPN GUI, aceste obiecte sunt: POliticile de securitate IP şi Conexiuni sigure. Astfel, când aceste informaţii se referă la un obiect , se referă la una sau mai multe dintre aceste părţi ale VPN.

Cele mai comune erori pe care le puteţi întâlni

Mesaj	**Simptom**
TCP5B28	Când încercaţi să activaţi reguli de filtrare pe o interfaţă, ajungeţi la acest mesaj: TCP5B28 CONNECTION_DEFINITION order violation
Articol negăsit	Când faceţi clic dreapta pe un obiect VPN şi selectaţi fie **Proprietăţi** sau **Ştergere**, ajungeţi la mesajul care spune **Articol negăsit**.
PARAMETER PINBUF IS NOT VALID	Când încercaţi să realizaţi o conexiune, ajungeţi la mesajul care spune **PARAMETER PINBUF IS NOT VALID...**
Articol de negăsit, server de chei la distanţă...	Când selectaţi **Proprietăţi** pentru o conexiune de chei dinamice, ajungeţi la o eroare care spune că serverul nu poate găsi serverul de chei la distanţă specificat de dumneavoastră.
Nu s-a putut actualiza obiectul	Când selectaţi **OK** pe foaia de proprietăţi pentru un grup de chei dinamice sau o conexiune manuală, ajungeţi la mesajul care vă spune că sistemul dumneavoastră nu poate actualiza obiectul.
Nu se poate cripta cheia...	Ajungeţi la mesajul care spune că sistemul nu poate encripta cheile dumneavoastră pentru că valoarea QRETSVRSEC trebuie să fie pusă pe 1.
CPF9821	Când încercaţi să expandaţi sau să deschideţi containerul Politici IP din Navigator iSeries(TM), apare mesajul CPF9821- Fără autorizare pentru programul QTFRPRS din biblioteca QSYS.

Alte probleme care pot apărea

Eroare	**Simptom**
Toate cheile sunt goale	Când vizualizaţi proprietăţile unei conexiuni manuale, toate cheile prepartajate şi cheile algoritmului pentru conexiune sunt goale.
O deschidere sesiune pentru un sistem diferit apare	Prima dată când folosiţi interfaţa de reguli pachete în Navigator iSeries, un ecran de deschidere de sesiune apare pentru un sistem diferit de cel curent.
Nici o stare de conexiune	O conexiune nu are valoarea în coloana **Stare** din fereastra Navigator iSeries.
Conexiunile oprite sunt încă active	După ce opriţi o conexiune, fereastra Navigator iSeries indică faptul că conexiunea este încă activă.
3DES nu este o alegere pentru criptare	Când lucraţi cu o transformare de politică IKE, transformare de politică de date sau o conexiune manuală, algoritmul de criptare 3DES nu este o alegere.
Afişare de coloane neaşteptată	Setaţi coloanele pe care vreţi să le afişaţi în fereastra Navigator iSeries pentru conexiunile dumneavoastră VPN; apoi, când vă uitaţi la ele mai târziu, vor fi afişate coloane diferite.

Regulile de filtrare active esuează dezactivarea	Când încercaţi să deactivaţi setul curent de reguli de filtrare, apare mesajul, Regulile active nu pot fi deactivate în fereastra de rezultate.
Grupul de chei dinamice pentru o conexiune se schimbă	Când creaţi o conexiune cu cheie dinamică, specificaţi un grup de chei dinamice şi un identificator pentru serverul de chei la distanţă. Mai târziu, când vedeţi proprietăţile obiectului conexiunii înrudite, pagina General a foii de proprietăţi afişează acelaşi identificator de server de chei la distanţă, dar un grup de chei dinamice diferit.

Mesaj de eroare VPN: TCP5B28

Simptome:
Când încercaţi să activaţi reguli de filtrare pe o anumită interfaţă, primiţi acest mesaj de eroare:

TCP5B28: Violare ordine CONNECTION_DEFINITION

Soluţia posibilă:
Regulile filtru pe care încercaţi să le activaţi conţineau definiţii de conexiune care au fost comandate diferit decât într-un set de reguli activat anterior. Cel mai uşor mod de a rezolva această eroare este de a activa fişierul cu reguli pe **toate interfeţele** în loc de o anumită interfaţă.

Mesaj de eroare VPN : Articolul nu a fost găsit

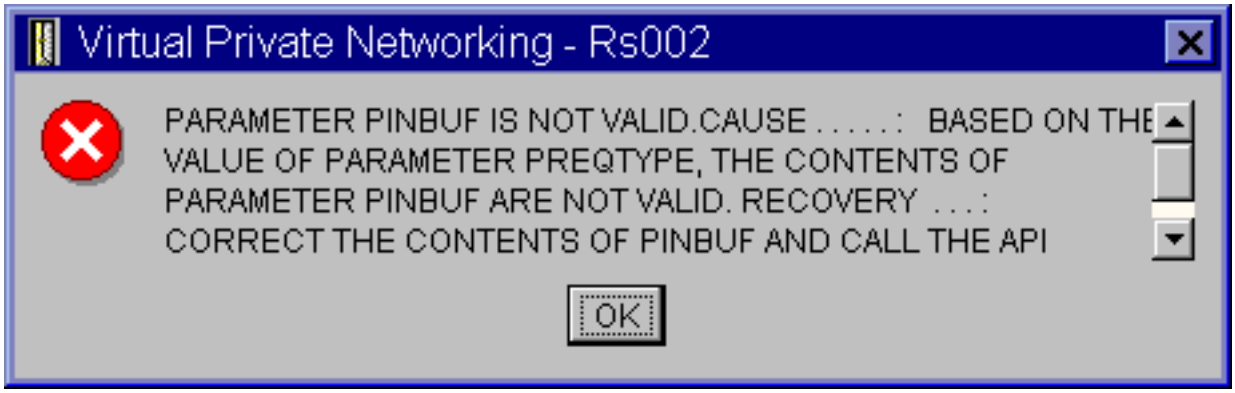
Simptome:
Când faceţi clic dreapta pe un obiect din fereastra Reţea privată virtuală şi selectaţi **Proprietăţi** sau **Ştergere**, apare mesajul următor:

Soluţia posibilă:

- Poate aţi şters sau redenumit obiectul şi nu aţi reîmprospătat încă fereastra. Ca urmare, obiectul apare încă în fereastra Reţea privată virtuală. Pentru a verifica dacă este aşa, din meniul **View**, selectaţi **Reîmprospătare**. Dacă obiectul apare tot în fereastra Reţea privată virtuală, continuaţi cu articolul următor din această listă.
- Când aţi configurat proprietăţile pentru obiect, s-ar putea să fi survenit o eroare de comunicaţie între serverul VPN şi iSeries(TM). Multe dintre obiectele care apar în fereastra Reţea privată virtuală au legătură cu mai mult de un obiect din baza de date a politicii VPN. Aceasta înseamnă că erorile de comunicaţie pot face ca unele obiecte din baza de date să fie legate de un obiect din VPN. De fiecare dată când creaţi sau actualizaţi un obiect, va apărea o eroare la pierderea sincronizării. Singurul mod de a rezolva problema este să selectaţi **OK** în fereastra de eroare. Aceasta lansează tabelul de proprietăţi al obiectului cu eroare. Doar câmpul de nume are o valoare în el. Toate celelalte sunt goale (sau conţin valori implicite). Introduceţi atributele corecte ale obiectului şi selectaţi **OK** pentru a salva schimbările.
- O eroare similară apare când încercaţi să ştergeţi obiectul. Pentru a rezolva această problemă, completaţi tabelul de proprietăţi gol care se deschide când faceţi clic pe **OK** în mesajul de eroare. Acesta actualizează orice legături la baza de date VPN care erau pierdute. Acum puteţi şterge obiectul.

Mesaj de eroare VPN: Parametrul PINBUF nu este valid

Simptome:
Când încercaţi să porniţi o conexiune, apare un mesaj ca următorul:



Soluţia posibilă:
Aceasta se întâmplă când sistemul este setat să folosească anumite localizări în care literele mici nu sunt mapate corect. Pentru a rezolva această eroare, asiguraţi-vă că toate obiectele folosesc numai litere mari sau schimbaţi localizarea sistemului.

Mesaj eroare VPN: Articolul nu a fost găsit, Server de chei la distanţă...

Simptome:
Când selectaţi **Proprietăţi** pentru o conexiune de chei dinamice, apare un mesaj ca următorul:

Soluţia posibilă:
Aceasta se întâmplă când creaţi o conexiune cu un anumit identificator de server de chei la distanţă şi apoi serverul de chei de la distanţă este şters din grupul său de chei dinamice. Pentru a ezolva această eroare, apăsaţi **OK** pe mesajul de eroare. Aceasta deschide foaia cu proprietăţi pentru conexiunea de chei dinamice care are eroarea. De aici, puteţi să adăugaţi serverul de chei la distanţă înapoi în grupul de chei dinamice sau selectaţi alt identificator server de chei la distanţă. Apăsaţi **OK** pe foaia de proprietăţi pentru a vă salva modificările.

Mesaj de eroare VPN: Nu se poate actualiza obiectul

Simptome:
Când selectaţi **OK** pe un table de proprietăţi pentru un grup de chei dinamice sau o conexiune manuală, apare următorul mesaj:

Soluţia posibilă:
Această eroare apare când o conexiune activă foloseşte obiectul pe care încercaţi să-l modificaţi. Nu puteţi modifica un obiect dintr-o conexiune activă. Pentru a modifica un obiect, identificaţi conexiunea activă corespunzătoare, apoi faceţi clic dreapta pe ea şi selectaţi **Oprire** din meniul contextual.

Mesaj de eroare VPN: Nu se poate cripta cheia...

Simptome:
Următorul mesaj de eroare apare:

Soluţia posibilă:
QRETSVRSEC este o valoare sistem care indică dacă sistemul poate memora cheile criptate pe el. Dacă această valoare este setată pe 0, atunci cheile prepartajate şi cheile pentru algoritmii dintr-o conexiune manuală nu pot fi memorate în baza de date a politicii VPN. Pentru a rezolva această problemă, folosiţi o sesiune de emulare 5250 către sistemul dumneavoastră. Tastaţi wrksysval în linia de comandă şi apăsaţi **Enter**. Căutaţi QRETSVRSEC în listă şi tastaţi 2 (modificare) lângă el. În panoul alăturat, tastaţi 1 şi apăsaţi **Enter**.

Mesaj de eroare VPN: CPF9821

Simptome:
Când încercaţi să expandaţi containerul Politici IP din Navigator iSeries(TM), apare mesajul CPF9821 - Neautorizat pentru programul QTFRPRS din biblioteca QSYS.

Soluţia posibilă:
Puteţi să nu aveţi autorizarea necesară pentru a extrage starea curentă a regulilor de pachete sau managerului de conexiune VPN. Asiguraţi-vă că aveţi autoritatea *IOSYSCFG pentru a căpăta acces la funcţiile regulă pachet din Navigatorul iSeries.

Eroare VPN: Toate cheile sunt goale

Simptome:
Toate cheile prepartajate şi cheile pentru algoritmi de conexiune manuală sunt goale.

Soluţia posibilă:
Aceasta se întâmplă când valoarea de sistem QRETSVRSEC este setată înapoi la 0. Setarea acestei valori de sistem la 0

şterge toate cheile din baza de date a politicii VPN. Pentru a rezolva această problemă trebuie să setaţi valoarea de sistem la 1 şi apoi să reintroduceţi toate cheile. Consultaţi Mesaj de eroare: Nu se pot cripta cheile pentru informaţii suplimentare despre cum se realizează aceasta.

Eroare VPN: Deschiderea unei sesiuni pentru un alt sistem apare când folosiţi Reguli pachet

Simptome:
Prima dată când folosiţi Reguli pachet, apare un ecran de deschidere de sesiune pentru un sistem diferit de cel curent.

Soluţia posibilă:
Reguli pachet foloseşte unicode pentru a memora regulile de securitate pachet în sistemul de fişiere integrat. Înregistrarea suplimentară permite Acces iSeries(TM) să obţină tabela de conversie corespunzătoare pentru unicode. Aceasta se va întâmpla doar o dată.

Eroare VPN: Starea conexiunii este goală în fereastra Navigator iSeries

Simptome:
O conexiune nu are nici o valoare în coloana **Stare** din fereastra Navigator iSeries(TM).

Soluţia posibilă:
Valoarea goală de stare arată că conexiunea este ăn curs de pornire. Adică nu este încă pornită, dar nu a întors încă o eroare. Atunci când reîmprospătaţi fereastra, conexiunea va afişa o stare de Eroare, Activă, La-cerere sau Inactivă.

Eroare VPN: Conexiunea a activat starea după ce aţi oprit-o

Simptome:
După ce opriţi o conexiune, fereastra Navigator iSeries(TM) indică dacă ea este încă activă.

Soluţia posibilă:
Aceasta se întâmplă de obicei pentru că nu aţi reîmprospătat fereastra Navigator iSeries încă. Astfel, fereastra conţine informaţii vechi. Pentru a repara aceasta, de la meniul **Vizualizare**, selectaţi **Reîmrpospătare**.

Eroare VPN : 3DES nu este o soluţie pentru criptare

Simptome:
Când lucraţi cu o tranformare de politică IKE, o transformare de politică de date sau cu o conexiune manuală, algoritmul de criptare 3DES nu este o alegere.

Soluţia posibilă:
Cel mai probabil, aveţi instalat doar produsul Cryptographic Access Provider AC2 (5722-AC2) pe sistemul dumneavoastră, nu Cryptographic Access Provider AC3 (5722-AC3). AC2 permite doar algoritmul de criptare DES (Data Encryption Standard), datorită restricţiilor la lungimile de cheie.

Eroare VPN: Afişare neaşteptată de coloane în fereastra Navigator iSeries

Simptome:
Setaţi coloanele pe care vreţi să le afişaţi în fereastra Navigator iSeries pentru conexiunile dumneavoastră VPN; apoi, când vă uitaţi la ele mai târziu, vor fi afişate coloane diferite.

Soluţia posibilă:
Când schimbaţi coloanele de vizualizat, schimbările nu sunt specifice unui anumit utilizator sau PC, ci mai degrabă, sunt pentru tot sistemul. Astfel, când altcineva schimbă coloanele din fereastră, schimbările afectează pe oricine vizualizează conexiunile de pe acel sistem.

Eroare VPN: Regulile de filtrare active nu pot fi deactivate

Simptome:
Când încercaţi să deactivaţi setul curent de reguli de filtrare, apare mesajul, Regulile active nu pot fi deactivate în fereastra de rezultate.

Soluţia posibilă:
De obicei, acest mesaj arată că există cel puţin o conexiune VPN activă. Trebuie să opriţi fiecare conexiune care starea activ. Pentru aceasta, faceţi clic dreapta pe fiecare conexiune activă şi selectaţi **Oprire**. Puteţi dezactiva acum regulile filtru.

Eroare VPN: Grupul de conexiune cheie pentru o conexiune se modifică

Simptome:
Când creaţi o conexiune cu cheie dinamică, specificaţi un grup de chei dinamice şi un identificator pentru serverul de chei la distanţă. Mai târziu, când selectaţi **Proprietăţi** pentru obiectul conexiune înrudit, pagina **General** a tabelului de proprietăţi afişează acelaşi identificator al serverului de chei la distanţă, dar un alt grup de chei dinamice.

Soluţia posibilă:
Identificatorul este singura informaţie memorată în baza de date a politicii VPN care se referă la serverul de chei la distanţă al conexiunii de chei dinamice. Când VPN verifică o politică pentru un server de chei la distanţă, caută primul grup de chei dinamice care are în el identificatorul serverului de chei dinamice la distanţă. Deci când vedeţi proprietăţile pentru una dintre aceste conexiuni, ea foloseşte acelaşi grup de chei dinamice găsit de VPN. Dacă nu doriţi să asociaţi grupul de chei dinamice cu acel server de chei dinamice, puteţi realiza una dintre următoarele acţiuni:

1. Înlăturaţi serverul de chei la distanţă din grupul de chei dinamice.
2. Expandaţi **După grupuri** în panoul din stânga al interfeţei VPN şi selectaţi şi trageţi grupul cheie dinamic pe care îl vreţi în vârful tabelei din panoul din dreapta. Aceasta asigură că VPN verifică întâi acest grup de chei dinamice pentru serverul de chei la distanţă.

Depanarea VPN cu jurnalul QIPFILTER

Jurnalul QIPFILTER se află în biblioteca QUSRSYS şi conţine informaţii despre seturi de reguli de filtrare, cât şi informaţii despre faptul dacă o datagramă IP a fost permisă sau respinsă. Înregistrarea în istoric se realizează pe baza opţiunii de jurnalizare pe care o specificaţi în regulile dumneavoastră de filtrare.

Cum să activaţi jurnalul Filtru Pachet IP
Utilizaţi editorul Reguli pachet din Navigator iSeries(TM) pentru a activa jurnalul QIPFILTER. Trebuie să activaţi funcţia de înregistrare în istoric pentru fiecare regulă filtru în parte. Nu există nici o funcţie care permite înregistrarea în jurnal pentru toate datagramele IP care intră sau ies din sistem.

Notă: Pentru a activa jurnalul QIPFILTER, filtrele dumneavoastră trebuie să fie dezactivate.

Următorii paşi descriu cum să activaţi jurnalizarea pentru o anumită regulă de filtrare:

1. În Navigator iSeries, expandaţi-vă serverul **—> Reţea—> Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Configurare**. Aeasta afişează interfaţa Reguli pachet.
3. Deschideţi un fişier cu reguli de filtrare existent.
4. Faceţi dublu clic pe regula de filtrare pe care doriţi s-o jurnalizaţi.
5. Pe pagina **General**, selectaţi **COMPLETĂ** în câmpul **Journalizare** ca în caseta de dialog de mai sus. Aceasta activează înregistrarea în jurnal pentru această regulă de filtrare.
6. Apăsaţi **OK**.
7. Salvaţi şi activaţi fişierul modificat cu regula de filtrare.

Dacă o datagramă IP se potriveşte cu definiţiile regulii de filtrare filter, este făcută o intrare în jurnalul QIPFILTER.

Cum să folosiţi jurnalul QIPFILTER
OS/400(R) Creează automat jurnalul prima oară când activaţi filtrarea pachet IP. Pentru a vedea detaliile specifice-intrării din jurnal, puteţi afişa intrările din jurnal pe ecran sau puteţi folosi un fişier de ieşire.

Copiind intrările din jurnal în fişierul de ieşire, puteţi vedea cu uşurinţă intrările folosind utilitare de interogare aşa cum este Query/400 sau SQL. Puteţi de asemenea să vă scrieţi propriile programe HLL pentru a procesa intrările din fişierele de ieşire.

Următorul este un exemplu de comandă Afişare Jurnal (DSPJRN):

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

Folosiţi următorii paşi pentru a copia intrările din jurnalul QIPFILTER în fişierul de ieşire:

1. Creaţi o copie a fişierului de ieşire furnizat de sistem QSYS/QATOFIPF într-o bibliotecă utilizator folosind comanda Creare Obiect Duplicat (CRTDUPOBJ). Următorul este un exemplu de comandă CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(bibliotecă)
        NEWOBJ(fişier)
   ```

2. Folosiţi comanda Afişare Jurnal (DSPJRN) pentru a copia intrările din jurnalul QUSRSYS/QIPFILTER în fişierul de ieşire pe care l-aţi creat în pasul anterior.

Dacă copiaţi DSPJRN într-un fişier de ieşire care nu există, sistemul creează un fişier pentru dumneavoastră, dar acesta nu conţine descrierile câmpului corecte.

Notă: Jurnalul QIPFILTER conţine doar intrări de permitere sau respingere pentru regulile filtru unde opţiunea de jurnalizare este setată pe COMPLETĂ. De exemplu, dacă setaţi doar reguli filtru PERMITERE, datagramele IP care nu sunt permise explicit sunt refuzate. Pentru aceste datagrame respinse, nici o intrare nu este la jurnal. Pentru analiza problemei puteţi să adăugaţi o regulă filtru care respinge în mod explicit orice alt trafic şi realizează jurnalizare COMPLETĂ. Apoi, veţi obţine intrările REFUZARE din jurnal pentru toate datagramele IP care sunt respinse. Din motive de performanţă, nu este recomandat să activaţi jurnalizarea pentru toate regulile filtru. O dată ce seturile dumneavoastră de filtrare sunt testate, reduceţi jurnalizarea la un subset de intrări folositor.

Vedeţi Câmpuri din jurnalul QIPFILTER pentru o tabelă care descrie fişierul de ieşire QIPFILTER.

Câmpurile din jurnalul QIPFILTER

Următoarea tabelă descrie câmpurile din fişierul de ieşire QIPFILTER:

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TFENTL	5	Y	Lungimea intrării	
TFSEQN	10	Y	Număr de ordine	
TFCODE	1	N	Cod jurnal	Întotdeauna M
TFENTT	2	N	Tip intrare	Întotdeauna TF
TFTIME	26	N	Marcă de timp SAA	
TFJOB	10	N	Nume job	
TFUSER	10	N	Profil utilizator	
TFNBR	6	Y	Număr job	
TFPGM	10	N	Nume program	
TFRES1	51	N	Rezervat	
TFUSPF	10	N	Utilizator	
TFSYMN	8	N	Nume sistem	
TFRES2	20	N	Rezervat	
TFRESA	50	N	Rezervat	
TFLINE	10	N	Descriere linie	*ALL dacă TFREVT este U* , spaţiu dacă TFREVT este L*, Nume linie dacă TFREVT este L
TFREVT	2	N	Eveniment regulă	L* sau L când regulile sunt încărcate. U* când regulile sunt descărcate, A la acţiune filtru

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TFPDIR	1	N	Direcţie pachet IP	O este ieşire, I este intrare
TFRNUM	5	N	Număr regulă	Se aplică la numărul regulii din fişierul activ de reguli
TFACT	6	N	Acţiunea filtru efectuată	PERMITERE, REFUZARE sau IPSEC
TFPROT	4	N	Protocol transport	1 este ICMP 6 este TCP 17 este UDP 50 este ESP 51 este AH
TFSRCA	15	N	Adresa IP sursă	
TFSRCP	5	N	Port sursă	Gunoi dacă TFPROT= 1 (ICMP)
TFDSTA	15	N	Adresa IP destinaţie	
TFDSTP	5	N	Port destinaţie	Gunoi dacă TFPROT= 1 (ICMP)
TFTEXT	76	N	Text suplimentar	Conţine descriere dacă TFREVT= L* sau U*

Depanare VPN cu jurnalul QVPN

VPN foloseşte un jurnal separat pentru a înregistra informaţiile despre trafic IP şi conexiuni numit jurnal QVPN. QVPN este memorat în biblioteca QUSRSYS. Codul jurnalului este M şi tipul jurnalului este TS. Veţi folosi rar intrările din jurnal zilnic. În schimb, s-ar putea să le găsiţi utile pentru depanarea şi verificarea că sistemul, cheile şi conexiunile dumneavoastră funcţionează în modul pe care l-aţi specificat. De exemplu, intrările jurnal vă ajută să înţelegeţi ce se întâmplă cu pachetele dumneavoastră de date. De asemenea vă ţin la curent cu starea curentă a VPN dumneavoastră

Cum să activaţi jurnalul VPN

Utilizaţi interfaţa reţea privată virtuală din Navigator iSeries(TM) pentru a activa jurnalul VPN. Nu există nici o funcţie care permite înregistrarea în jurnal pentru toate conexiunile VPN. De aceea, trebuie să activaţi funcţia de înregistrare în istoric pentru fiecare grup cheie dinamic sau conexiune manuală.

Următorii paşi descriu cum să activaţi funcţia de jurnalizare pentru un anumit grup de chei dinamice sau conexiune manuală:

1. În Navigator iSeries, expandaţi-vă serverul **—> Reţea—> Politici IP—> Reţea privată virtuală—> Conexiuni sigure.**
2. Pentru grupuri de chei dinamice, expandaţi **După grup** şi apoi faceţi clic dreapta pe grupul de chei dinamice pentru care doriţi să activaţi jurnalizarea şi selectaţi **Proprietăţi.**
3. Pentru conexiuni manuale, expandaţi **Toate conexiunile** şi apoi faceţi clic dreapta pe conexiunea manuală pentru care doriţi să activaţi jurnalizarea.
4. În pagina **General**, selectaţi nivelul de jurnalizare pe care îl cereţi. Aveţi de ales dintre patru opţiuni. Acestea sunt:
   Nici una
   Nu apare nici o jurnalizare pentru acest grup de conexiuni.
   Toate
   Jurnalizarea se realizează pentru toate activităţile conexiunii, cum ar fi pornirea sau oprirea unei conexiuni sau reîmprospătarea unei chei, cât şi pentru informaţiile despre traficul IP.
   Activitate conexiune

Jurnalizarea se realizează pentru o activitate a conexiunii, cum ar fi pornirea sau oprirea unei conexiuni.
Trafic IP
Jurnalizarea se realizează pentru tot traficul VPN care este asociat cu această conexiune. Este făcută o intrare în jurnal de fiecare dată când o regulă filtru este invocată. Sistemul înregistrează informaţii despre traficul IP în jurnalul QIPFILTER, care se află în biblioteca QUSRSYS.

5. Apăsaţi **OK**.
6. Porniţi conexiunea pentru a activa jurnalizarea.

Notă: Înainte de a putea opri jurnalizarea, asiguraţi-vă că conexiunea este inactivă. Pentru a schimba starea jurnalizării unui grup de conexiuni, asiguraţi-vă că nu sunt conexiuni active asociate cu acel grup.

Cum să folosiţi jurnalul VPN
Pentru a vedea detaliile specifice-intrării din jurnalul VPN, puteţi afişa intrările din jurnal pe ecran sau puteţi folosi un fişier de ieşire.

Copiind intrările din jurnal în fişierul de ieşire, puteţi vedea cu uşurinţă intrările folosind utilitare de interogare aşa cum este Query/400 sau SQL. Puteţi de asemenea să vă scrieţi propriile programe HLL pentru a procesa intrările din fişierele de ieşire. Următorul este un exemplu de comandă Afişare Jurnal (DSPJRN):

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

Folosiţi următorii paşi pentru a copia intrările din jurnalul VPN în fişierul de ieşire:

1. Creaţi o copie a fişierului de ieşire furnizat de sistem QSYS/QATOVSOF într-o bibliotecă utilizator. Puteţi face aceasta folosind comanda Creare Obiect Duplicat (CRTDUPOBJ). Următorul este un exemplu de comandă CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(bibliotecă)
        NEWOBJ(fişier)
   ```

2. Folosiţi comanda Afişare Jurnal (DSPJRN) pentru a copia intrările din jurnalul QUSRSYS/QVPN în fişierul de ieşire pe care l-aţi creat în pasul anterior. Dacă încercaţi să copiaţi DSPJRN într-un fişier de ieşire care nu există, sistemul creează un fişier pentru dumneavoastră, dar acesta nu conţine descrierile câmpului corecte.

Vedeţi Câmpuri jurnal QVPN pentru o tabelă care descrie câmpurile din fişierul de ieşire QVPN.

Câmpurile din jurnalul QVPN

Următoarea tabelă descrie câmpurile din fişierul de ieşire QVPN:

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TSENTL	5	Y	Lungimea intrării	
TSSEQN	10	Y	Număr de ordine	
TSCODE	1	N	Cod jurnal	Întotdeauna M
TSENTT	2	N	Tip intrare	Întotdeauna TS
TSTIME	26	N	Marca de timp a intrării SAA	
TSJOB	10	N	Numele jobului	
TSUSER	10	N	Utilizatorul jobului	
TSNBR	6	Y	Numărul jobului	
TSPGM	10	N	Numele programului	
TSRES1	51	N	Nefolosit	
TSUSPF	10	N	Nume profil utilizator	
TSSYNM	8	N	Nume sistem	
TSRES2	20	N	Nefolosit	

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TSRESA	50	N	Nefolosit	
TSESDL	4	Y	Lungimea datelor specifice	
TSCMPN	10	N	Componenta VPN	
TSCONM	40	N	Nume conexiune	
TSCOTY	10	N	Tip conexiune	
TSCOS	10	N	Stare conexiune	
TSCOSD	8	N	Data de pornite	
TSCOST	6	N	Timpul pornirii	
TSCOED	8	N	Data de sfârşit	
TSCOET	6	N	Timpul de sfârşit	
TSTRPR	10	N	Protocol transport	
TSLCAD	43	N	Adresa locală a clientului	
TSLCPR	11	N	Porturi locale	
TSRCAD	43	N	Adresa de la distanţă a clientului	
TSCPR	11	N	Porturi de la distanţă	
TSLEP	43	N	Punct final local	
TSREP	43	N	Punct final la distanţă	
TSCORF	6	N	Număr de reîmprospătări	
TSRFDA	8	N	Data următoarei reîmprospătări	
TSRFTI	6	N	Timpul următoarei reîmprospătări	
TSRFLS	8	N	Durata de viaţă a reîmprospătării	
TSSAPH	1	N	Faza SA	
TSAUTH	10	N	Tip autentificare	
TSENCR	10	N	Tip criptare	
TSDHGR	2	N	Grup Diffie-Hellman	
TSERRC	8	N	Cod eroare	

Depanarea VPN cu jurnalul VPN

Când aveţi probleme la conexiunile dumneavoastră VPN, este întotdeauna recomandabil să analizaţi jurnalele. De fapt există câteva jurnale care conţin mesaje de eroare şi alte informaţii legate de un mediu VPN.

Este important să analizaţi istoricurile de joburi din ambele părţi ale conexiunii dacă ambele sunt servere iSeries(TM). Când o conexiune dinamică nu poate porni, este folositor să înţelegeţi ce se întâmplă pe serverul de la distanţă.

Joburile VPN, QTOVMAN şi QTOKVPNIKE, rulează în subsistemul QSYSWRK. Puteţi vedea istoricurile de joburi respective din Navigatorul iSeries OS/400(R).

Această secţiune prezintă cele mai importante sarcini pentru un mediu VPN. Lista următoare arată numele jobului şi o scurtă explicaţie a utilităţii jobului:

QTCPIP
Acest job este jobul de bază care portneşte toate interfeţele TCP/IP. Dacă aveţi probleme fundamentale cu TCP/IP în general, analizaţi jurnalul QTCPIP.

QTOKVPNIKE
Jobul QTOKVPNIKE este jobul de gestiune a managerului de chei VPN. Managerul de chei VPN ascultă pe portul UDP 500 pentru a realiza procesarea protocolului IKE.

QTOVMAN
Acest job este managerul de conexiuni pentru conexiunile VPN. Jurnalul asociat conţine mesaje pentru fiecare încercare de conectare care eşuează.

QTPPANSxxx
Acest job este folosit pentru conexiuni dial-up PPP. El răspunde la încercări de conectare unde *ANS este definit într-un profil PPP.

QTPPPCTL
Acesta este un job PPP pentru conexiuni prin apelare telefonică.

QTPPPL2TP
Acesta este jobul de gestionare a Layer Two Tunneling Protocol (L2TP). Dacă aveţi probleme la configurarea unui tunel L2TP, vedeţi mesajele din acest jurnal.

Mesaje de eroare comune ale managerului de conexiune VPN
Această secţiune descrie câteva dintre cele mai obişnuite mesaje de eroare ale managerului de conexiune pe care le puteţi întâlni.

În general, managerul de conexiune VPN reţine două mesaje în jurmalul de joburi QTOVMAN când o eroare apare cu o conexiune VPN. Primul mesaj furnizează detalii cu privire la eroare. Puteţi vedea informaţii despre aceste erori în Navigatorul iSeries(TM) făcând clic dreapta pe conexiunea cu eroare şi selectând **Informaţii eroare**.

Al doilea mesaj descrie acţiunea pe care aţi încercat-o pentru această conexiune când a apărut eroarea. De exemplu, pornirea sau oprirea ei. Mesajele TCP8601, TCP8602 şi TCP860A, descrie mai jos, sunt exemple tipice de mesaje secundare din acestea.

Mesajele de eroare ale managerului de conexiune VPN

Mesaj	Cauză	Recuperare
TCP8601 Nu s-a putut porni conexiunea VPN [*nume conexiune*]	Nu s-a putut porni această conexiune VPN datorită unui sau mai multe coduri motiv: *0* - Un mesaj anterior din jurnalul de joburi cu acelaşi nume de conexiune VPN are mai multe informaţii detaliate. *1* - Configurarea politicii VPN. *2* - Eşuarea reţelei de comunicaţii. *3* - Managerul de chei VPN a eşuat în a negocia o nouă asociere de securitate. *4* - Punctul final la distanţă pentru această conexiune nu este configurat corespunzător. *5* - Mangarul de chei VPN a eşuat să raspundă managerului de conexiune VPN. *6* - Eşuare de încărcare a conexiunii VPN a componentei de securitate IP. *7* - Eşuare componentă PPP.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi Navigator iSeries pentru a vizualiza starea conexiunii. Conexiunile care nu au putut fi pornite for fi în stare de eroare.

Mesaj	Cauză	Recuperare
TCP8602 Eroarea a apărut la oprirea conexiunii VPN [*nume conexiune*]	Conexiunea VPN specificată a fost cerutp închisă, oricum, nu s-a oprit sau s-a oprit în eroare datorită codului motiv : *0* - Un mesaj anterior din jurnalul de joburi cu acelaşi nume de conexiune VPN are mai multe informaţii detaliate. *1* - Conexiunea VPN nu există. *2* - Eşuare de comunicaţii internă cu managerul de chei VPN. *3* - Eşuare de comunicaţii internă cu componenta IPSec. *4* - Eşuare de comunicaţii cu punctul final la distanţă de conexiune VPN.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi Navigator iSeries pentru a vizualiza starea conexiunii. Conexiunile care nu au putut fi pornite for fi în stare de eroare.
TCP8604 Pornire eşuată a conexiunii VPN [*nume conexiune*]	O pornire a acestei conexiuni VPN a eşuat datorită unuia din următoarele coduri eroare: *1* - Nu s-a putut translata numele gazdă la distanţă la o adresă IP. *2* - Nu s-a putut translata numele gazdă locală la o adresă IP. *3* - Regula de filtrare a politicii VPN asociată cu această conexiune VPN nu este încărcată. *4* - O valoare de cheie specificată de utilizator nu este validă pentru algoritmul asociat ei. *5* - Valoarea iniţială pentru conexiunea VPN nu permite specificarea acţiunii. *6* - Un rol sistem pentru conexiunea VPN este inconsistent în informaţii de la grupul de conexiune. *7* - Rezervat. *8* - Punctele finale de date (servicii şi adrese la distanţă şi locale) a acestei conexiuni VPN sunt inconsistente în informaţii de la grupul de conexiune. *9* - Tipul identificator nu este valid.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi Navigator iSeries pentru a verifica sau corecta configuraţia de politică VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.
TCP8605 Managerul de conexiune VPN nu a putut să comunice cu managerul de chei VPN	Managerul de conexiune VPN necesită serviciile managerului de chei VPN pentru a stabili asocierile de securitate pentru conexiunile VPN dinamice. Managerul de conexiune VPN nu a putut să comunice cu managerul de chei VPN.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Verificaţi dacă interfaţa *LOOPBACK este activă folosind comanda NETSTAT OPTION(*IFC). 3. Terminaţi serverul VPN folosind comanda ENDTCPSVR SERVER(*VPN). Apoi reporniţi serverul VPN folosind comanda STRTCPSRV SERVER(*VPN). **Notă:** Aceasta provoacă toate conexiunile VPN să se termine.

Mesaj	Cauză	Recuperare
TCP8606 MAnagerul de chei VPN nu a putut stabili asocierea de securitate cerută pentru conexiune, [*nume conexiune*]	Managerul de chei VPN nu a putut stabili asocierea de securitate cerută datorită unuia din următoarele coduri eroare: *24* - Eşuarea autentificării cheii conexiunii Managerului de chei VPN. *8300* - Eşuarea a apărut în timpul negocierilor de chei ale conexiunii managerului de chei VPN. *8306* - Nu s-a găsit nici o cheie prepartajată. *8307* - Nu s-a găsit nici o politică de fază 1 IKE la distanţă. *8308* - Nu s-a găsit nici o cheie prepartajată la distanţă. *8327* - E expirat timpul negocierilor de chei de conexiune a managerului de chei VPN. *8400* - Eşuare apărută în timpul negocierilor de conexiune VPN ale managerului de chei Key VPN. *8407* - Nu s-a găsit nici o politică de fază 2 IKE la distanţă. *8408* - E expirat timpul de negocieri de conexiune VPN ale managerului de chei VPN. *8500 sau 8509* - A apărut o eroare de reţea la managerul de chei VPN.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi Navigator iSeries pentru a verifica sau corecta configuraţia de politică VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.
TCP8608 Conexiunea VPN, [*nume conexiune*], nu a putut obţine o adresă NAT.	Acest grup de chei dinamice sau conexiune de date au specificat că translatarea de adresă reţea (NAT) e făcută pe una sau mai multe adrese şi că a eşuat datorită unuia dintre posibilele coduri motiv: *1* - Adresa pe care se aplică NAT nu este o singură adresă IP. *2* - Toate adresele disponibile au fost folosite.	1. Verificaţi jurnalul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi Navigator iSeries pentru a verifica sau corecta politica VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile pentru adrese.
TCP8620 Nu este disponibil punctul final de conexiune local.	Nu s-au putut activa aceste conexiuni VPN pentru că punctul final de conexiune locală nu a fost disponibil.	1. Verficaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Asiguraţi-vă că punctul final de conexiune local este definit şi pornit folosid comanda NETSTAT OPTION(*IFC). 3. Corectaţi orice erori şi încercaţi cererea din nou.

Mesaj	Cauză	Recuperare
TCP8621 Punct final de date local disponibil	Nu s-a putut activa această conexiune VPN pentru că punctul final de date local nu a fost disponibil.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Asiguraţi-vă că punctul final de conexiune local este definit şi pornit folosid comanda NETSTAT OPTION(*IFC). 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8622 încapsularea de transport nu este permisă cu un gateway	Nu s-a putut activa această conexiune VPN pentru că politica negociată a specificat modul de încapsulare de transport şi această conexiune este definită ca un gateway de securitate.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a schimba politica VPN asociată cu această conexiune VPN. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8623 Conexiunea VPN se supreapune cu una existentă	Nu s-a putut activa această conexiune VPN pentru că o conexiune VPN existentă este deja activată. Această conexiune are un punct final de date local de [*valoarea punctului final de date local*] şi un punct final de date la distanţă de [*valoarea punctutlui final de date la distanţă*].	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a vizualiza toate conexiunile activate care au puncte finale de date locale şi puncte finale de date la distanţă care se suprapun peste conexiune. Schimbaţi politica unei conexiuni existente dacă amndouă conexiunile sunr necesare. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8624 Conexiunea VPN nu este în domeniul regulii de filtrare a politii asociate	Nu s-a putut activa această conexiune VPN pentru că punctele finale de date nu sunt în regula de filtrare a politicii definite.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a afişa restricţiile de punc final de date pentru această conexiune sau grup de chei dinamice. Dacă **Subset de filtru de politică** sau **Personalizarea de potrivire a filtrului de politici** este selectat, atunci verificaţi punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acţiune IPSEC şi un nume de conexiune VPN asociat cu această conexiune. Schimbaţi politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Mesaj	Cauză	Recuperare
TCP8625 Conexiunea VPN e eşuat o verificare de algoritm ESP	Nu s-a putut activa această conexiune VPN din cauza insuficienţei cheii secrete asociată cu conexiunea.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a afişa politica asociată cu această conexiune şi introduceţi o cheie secretă diferită. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8626 Punctul final al conexiunii VPN n ueste acelaşi cu punctul final de date.	Nu s-a putut activa această conexiune VPN pentru că politica specifică o gazdă existentă şi punctul final de conexiune VPN nu este acelaşi lucru cu punctul final de date.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a afişa restricţiile de punc final de date pentru această conexiune sau grup de chei dinamice. Dacă **Subset de filtru de politică** sau **Personalizarea de potrivire a filtrului de politici** este selectat, atunci verificaţi punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acţiune IPSEC şi un nume de conexiune VPN asociat cu această conexiune. Schimbaţi politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8628 Regula de filtrare politici nu este încărcată	Regula de filtrare politici pentru această conexiune nu este acivă.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a afişa filtrele de politici active. Verificaţi regula de filtrare politici pentru această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8629 Pachet IP abandonat pentru conexiunea VPN	Această conexiune VPN are VPN NAT configurat şi setul cerut de adrese NAT a depăşit adresele disponibile NAT.	1. Verificaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi Navigator iSeries pentru a creşte numărul de adrese NAT atribuite pentru această conexiune VPN. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Mesaj	Cauză	Recuperare
TCP862A Conexiunea PPP e eşuat pornirea	Această conexiune VPN a fost asociată cu un profil PPP. Când a fost pornit, a fost făcută o încercare de pornire a profilului PPP, dar o eşuare a apărut.	1. Verficaţi jurnalele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Verificaţi jurnalul de joburi asociat cu conexiunea PPP. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Depanarea VPN cu urmărirea comunicaţiilor OS/400

iSeries(TM) OS/400(R) furnizează capabilitatea de urmărire a datelor pe o linie de comunicaţie, cum ar fi o interfaţă reţea locală (LAN) sau reţea pe zonă extinsă (WAN). Utilizatorul mijlociu poate să nu înţeleagă întregul conţinut al datelor de urmărire. Oricum, puteţi folosi intrările de urmărire pentru a determina dacă un schimb de date între sistemele la distanţă şi local a avut loc.

Pornirea urmăririi de comunicaţii

Folosiţi comanda de pornire urmărire comunicaţii (STRCMNTRC) pentru a porni urmărirea de comunicaţii de pe sistemul dumneavoastră. Ceea ce urmează este un exemplu al comenzii STRCMNTRC:

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

Parametrii de comandă sunt explicaţi în lista următoare:

CFGOBJ (Obiectul de configurare)
Numele obiectului de configuraţie de urmărit. Obiectul este fie o descriere de linie, o descriere de interfaţă reţea sau o descriere de server reţea.

CFGTYPE(Tip configurare)
Când o linie (*LIN), o interfaţă de reţea (*NWI) sau un server de reţea (*NWS) este urmărit.

MAXSTG (Dimensiune buffer)
Dimensiunea bufferului necesar urmăririi. Valoarea implicită este setată la 128 KB. Intervalul merge de la 128 KB la 64 MB. Dimensiunea maximaă actuală a bufferului a sistemului de întindere mare este definit în Uneltele de servicii sistem (SST). De aceea, puteţi primi un mesaj de eroare când se foloseşte o dimensiune de buffer mai mare la comanda STRCMNTRC decât cea definită în SST. Ţineţi minte că suma dimensiunilor de buffer specificate pe toate urmăririle de comunicaţii pornite nu trebuie să depăşească dimensiunea maximă de buffer definită în SST.

DTADIR (Direcţia de date)
Direcţia traficului de date de urmărit. Direcţia poate fi doar trafic de ieşire (*SND), doar trafic de intrare (*RCV) sau ambele (*BOTH).

TRCFULL (Urmărire plină)
Ce apare când bufferul de urmărire este plin. Acest parametru are două posibile valori. Valoarea implicită este *WRAP, care înseamnă, când buffer de urmărire este plin, că urmărirea se îmbrobodeşte de la început. Cele mai vechi înregistrări de urmărire scrise peste cele noi după cum sunt colectate.

A doua valoare *STOPTRC lasă urmărirea oprită când bufferul de urmărire, specificat în parametrul MAXSTG, este plin de înregistrări de urmărire. Ca o regulă generală, meereu să definiţi dimensiunea bufferului astfel încât să fie suficient de mare ca să reţină toate înregistrările de de urmărire. Dacă urmărirea se derulează la început, puteţi pierde informaţii importante de urmărire. Dacă experimentaţi o problemă de intermitenţă înaltă, definiţi bufferul de urmărire să fie destul de mare astfel ca o derulare a bufferului să nu abandoneze informaţii importante.

USRDTA (Numărul de octeţi utilizator de urmărit)
Defineşte numărul de date de urmărit în partea de date utilizator a cadrelor de date. Implicit doar primii 100 de octeţi de date utilizator sunt capturate pentru interfeţele LAN. Pentru toate celelalte interfeţe, toate datele utilizator sunt capturate. Asiguraţi-vă că specificaţi *MAX dacă suspectaţi probleme în datele utilizator a unui cadru.

TEXT (Descrierea de unrmărire)
Furnizează o descriere cu sens a urmăririi.

Oprirea urmăririi de comunicaţii
Dacă nu specificaţi altfel, urmărirea se opreşte tipic în momentul în care apare condiţia pe care o urmăriţi. Folosiţi comanda de terminare urmărire de comunicaţii (ENDCMNTRC) pentru a opri urmărirea. Următoarea comandă este un exemplu de comandă ENDCMNTRC:

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

Comanda are doi parametrii:

CFGOBJ (Obiectul de configurare)
Numele obiectului de configurare pentru care urmărirea rulează. Obiectul este fie o descriere de linie, de interfaţă reţea sau de server reţea.

CFGTYPE (Tip de configurare)
Când o linie (*LIN), o interfaţă de reţea (*NWI) sau un server de reţea (*NWS) este urmărit.

Tipărirea datelor de urmărire
După ce aţi oprit urmărirea de comunicaţii, trebuie să tipăriţi datele de urmărire. Folosiţi comanda de tipărire a urmărire de comunicaţii (PRTCMNTRC) pentru a executa această operaţie. Atât timp cât tot traficul de linii este capturat în perioada de urmărire, aveţi opţiuni de filtrare multiple pentru genearea ieşirii. Încercaţi să păstraţi fişierul spooled pe cât de mic posibil. Acesta face analiza mai repede şi mai eficient. În cazul unei probleme VPN, filtraţi doar în traficul IP şi, dacă e posibil, într-o adresă IP specifică. Aveţi opţiunea de filtrare pe un număr de port IP anume. Ceea ce urmează este un exemplu de comandă PRTCMNTRC:

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

În acest exemplu, urmărirea este formatată pentru trafic IP şi conţine doar date pentru adresa IP, unde adresa sursă şi destinaţie este 10.50.21.1 şi numărul de port IP destinaţie sau sursă este 500.

Doar cei mai importanţi parametrii ai comenzii pentru analizarea de probleme VPN, sunt explicaţi mai jos:

CFGOBJ (Obiectul de configurare)
Numele obiectului de configurare pentru care urmărirea rulează. Obiectul este fie o descriere de linie, de interfaţă reţea sau de server reţea.

CFGTYPE (Tip configurare)
E urmărită o linie (*LIN), o interfaţă reţea (*NWI) sau un server de reţea (*NWS).

FMTTCP (Format de date TCP/IP)
Dacă se formatează urmărirea pentru datele TCP/IP şi UDP/IP. Specificaţi *YES pentru a formata urmărirea pentru datele IP.

TCPIPADR (Formatul de date TCP/IP prin adresă)
Acest parametru conţine două elemente. Dacă specificaţi adresele IP pe fiecare element, doar traficul IP între acele adrese vor tipări.

SLTPORT (Numărul de port IP)
NUmărul de port IP de filtrare.

FMTBCD (Format de date broadcast)
Dacă toate cadrele de broadcast sunt tipărite. Valoarea implicită este Da. Dacă nu vreţi; de exemplu, cererile de protocol de rezoluţie de adrese (ARP), specificaţi *NO; altfel puteţi fi depăşit cu mesaje de tip broadcast.

Informaţii înrudite pentru VPN

Pentru mai multe scenarii şi descrieri de configuraţii VPN, consultaţi aceste surse de informaţii:

- **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**

  Acest manual IBM oferă un proces pas cu pas pentru configurarea tunelului VPN folosind VPN din V5R1 şi suportul L2TP şi IPSec integrat în Windows 2000.
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  Acest manual explorează conceptele VPN şi descrie implementarea folosind securitate IP (IPSec) şi Layer 2 Tunneling Protocol (L2TP) pe OS/400.
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  Acest manual explorează toate caracteristicile de securitate integrată disponibile pe sistemul OS/400 cum ar fi flitre IP, NAT, VPN, server proxy HTTP, SSL, DNS, retransmitere mail, auditare şi întregistrare în istoric. Descrie utilizarea lor prin exemple practice.
- **Virtual Private Networking: Securing Connections**

  Această pagină Web conţine ştiri recente despre VPN, liste cu cele mai noi PTF-uri şi legături la alte situri de interes.
- **Alte manuale şi cărţi Redbooks legate de securitate**
  Mergeţi aici pentru o listă de informaţii legate de securitate disponibile online.

Pentru a salva un PDF pe staţia dumneavoastră de lucru pentru citire sau tipărire:

1. Faceţi clic dreapta pe PDF în browser (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe **Save Target As...**.
3. Deplasaţi-vă la directorul în care vreţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

Dacă aveţi nevoie de Adobe Acrobat Reader pentru a citi sau a tipări aceste PDF-uri, puteţi descărca o copie de pe Situl Web Adobe (www.adobe.com/prodindex/acrobat/readstep.html)

.

Anexa. Observaţii

Această publicaţie a fost elaborată pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentanţa IBM locală pentru a obţine informaţii cu privre la produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licenţa pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

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

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte character set), contactaţi departamentul de proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

Paragraful următor nu este valabil în cazul Marii Britanii sau al altor ţări în care asemenea prevederi sunt incompatibile cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE SUBÎNŢELESE DE NEÎNCĂLCARE, COMERCIALIZARE SAU POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau deduse în anumite tranzacţii, de aceea este posibil ca această declaraţie să nu fie valabilă în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie pentru dumneavoastră.

Posesorii de licenţă pentru acest program care doresc să obţină informaţii despre el cu scopul de a realiza: (i) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (ii) utilizarea mutuală a informaţiilor care au fost schimbate, trebuie să contacteze:

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

Aceste informaţii pot fi făcute disponibile în conformitate cu anumiţi termeni şi condiţii, iar în unele cazuri după plata unei taxe.

Programul cu licenţă descris în această publicaţie şi toate materialele cu licenţă disponibile pentru el sunt furnizate de IBM în conformitate cu termenii din Contracul IBM cu Clientul, Contractul IBM de Licenţă Internaţională pentru Program sau oricare alt contract echivalent încheiat între noi.

Datele de performanţă prezentate aici au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de operare pot varia semnificativ. Anumite măsurători s-ar putea să fi fost făcute pe sisteme în faza de dezvoltare şi nu este nici o garanţie că aceste măsurători vor da aceleaşi rezultate pe sistemele disponibile pe piaţă. Mai mult, unele măsurători s-ar putea să fi fost realizate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse publice. IBM nu a testat aceste produse şi nu poate confirma nivelul performanţei, compatibilităţii sau al oricăror altor pretinse calităţi legate de produsele non-IBM. Întrebările legate de capabilităţile produselor non-IBM trebuie să fie adresate furnizorilor acestor produse.

Toate declaraţiile referitoare la direcţia sau intenţiile viitoare ale IBM pot fi modificate sau retrase fără notificare, ele reprezentând doar nişte obiective.

Toate preţurile IBM afişate sunt preţuri de vânzare cu amănuntul sugerate de IBM; ele reprezintă valori curente şi pot fi modificate fără notificare. Preţurile dealer-ilor pot varia.

Aceste informaţii sunt doar pentru planificare. Informaţiile oferite aici pot fi modificate înainte ca produsele descrise să devină disponibile.

Aceste informaţii conţin exemple de date şi raporturi folosite în operaţiile zilnice din companie. Pentru a le ilustra cât mai complet posibil, exemplele includ numele de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu numele şi adresele folosite de o întreprindere de afaceri reală este complet întâmplătoare.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance şi WordPro sunt mărci comerciale deţinute de International Business Machines Corporation şi Lotus Development Corporation în Statele Unite, în alte ţări sau ambele.

C-bus este o marcă comercială deţinută de Corollary, Inc. în Statele Unite, în alte ţări sau ambele.

ActionMedia, LANDesk, MMX, Pentium şi ProShare sunt mărci comerciale sau mărci comerciale înregistrate deţinute de Intel Corporation în Statele Unite, în alte ţări sau ambele.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci înregistrate deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

SET şi logo-ul SET sunt mărci comerciale deţinute de SET Secure Electronic Transaction LLC.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată deţinută de The Open Group în Statele Unite şi în alte ţări.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau de servicii ale altora.

Termeni şi condiţii pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru utilizarea publicaţiilor pe care le-aţi selectat pentru descărcare sunt acordate ca urmare a termenilor şi condiţiilor următoare şi a indicaţiei dumneavoastră de acceptare a lor.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru uzul dumneavoastră personal, necomercial cu condiţia să fie păstrate toate observaţiile privind proprietatea. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Uz comercial: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate observaţiile privind proprietatea să fie păstrate. Nu puteţi realiza derivate ale acestor publicaţii sau să reproduceţi, să distribuiţi sau să afişaţi aceste publicaţii sau o porţiune din ele în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit în această permisiune, nici o altă permisiune, licenţă sau drept nu vor mai fi acordate, explicit sau implicit, asupra publicaţiilor sau a altor informaţii, date, software sau altă proprietate intelectuală conţină aici.

IBM îşi rezervă dreptul de a retrage aceste permisiuni acordate aici oricând, în opinia sa, utilizarea publicaţiilor nu este în interesul său sau, instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau rexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite. IBM NU OFERĂ GARANŢII DESPRE CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE SUNT FURNIZATE ″AŞA CUM SUNT″ ŞI FĂRĂ GARANŢIE DE NICI UN FEL, FIE EXPLICITĂ, FIE IMPLICITĂ, INCLUSIV DAR NU LIMITAT LA GARANŢIILE IMPLCITE DE MERCANTIBILITATE ŞI POTRIVIRE PENTRU UN SCOP PARTICULAR.

Pentru toate materialele există copyright al IBM Corporation.

Prin descărcarea sau tipărirea unei publicaţii de pe acest sit, aţi indicat că sunteţi de acord cu aceşti termeni şi condiţii.

Tipărit în S.U.A.