



IBM Systems - iSeries
VPN (Virtual Private Networking)

Versiunea 5 Ediția 4





IBM Systems - iSeries

VPN (Virtual Private Networking)

Versiunea 5 Ediția 4

Notă

Înainte de a utiliza aceste informații și produsul pe care îl suportă, citiți informațiile din “Observații”, la pagina 75.

Ediția a șaptea (februarie 2006)

Această ediție se aplică versiunii 5, ediția 4, modificarea 0 a IBM i5/OS (număr produs 5722-SS1) și tuturor edițiilor și modificărilor ulterioare, până când se indică altceva în edițiile noi. Această versiune nu rulează pe toate modelele RISC (reduced instruction set computer), nici pe modelele CISC.

© Copyright International Business Machines Corporation 1998, 2006. Toate drepturile rezervate.

Cuprins

| | | | |
|---|----------|---|-----------|
| VPN (Virtual Private Networking) | 1 | Configurarea unei conexiuni manuale | 45 |
| Ce este nou pentru V5R4 | 1 | Configurarea regulilor de pachete VPN | 46 |
| PDF tipăribil | 2 | Configurarea TFC (Traffic Flow Confidentiality) | 51 |
| Conceptele VPN. | 2 | Configurarea ESN (Extended Sequence Number) | 51 |
| Protocoalele IP Security (IPSec) | 2 | Pornirea unei conexiuni VPN | 51 |
| Gestionarea cheilor | 6 | Administrarea VPN | 52 |
| Layer 2 Tunnel Protocol (L2TP) | 8 | Setarea atributelor implicite pentru conexiunile dumneavoastră | 52 |
| Translatarea adreselor de rețea pentru VPN. | 9 | Resetarea conexiunilor în starea de eroare | 52 |
| IPSec compatibil NAT cu UDP | 10 | Vizualizarea informației de eroare | 52 |
| Comprimarea IP (IPComp) | 11 | Vizualizarea atributelor conexiunilor active | 52 |
| VPN și filtrarea IP. | 12 | Folosirea urmării serverului VPN (VPN server trace) | 53 |
| Scenarii VPN | 13 | Vizualizarea fișierelor jurnal job ale serverului VPN. | 53 |
| Scenariu: Conexiunea de bază cu biroul filialei | 13 | Vizualizarea atributelor Asocierilor de securitate (Security Associations - SA). | 54 |
| Scenariu: Conexiunea de bază companie la companie | 17 | Oprirea unei conexiuni VPN. | 54 |
| Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec | 22 | Ștergerea obiectelor de configurare VPN | 54 |
| Scenariu: VPN prietenos pentru firewall | 28 | Depanarea VPN | 54 |
| Scenariu: Folosirea translatării adreselor de rețea pentru VPN | 33 | Inițierea în depanarea VPN | 54 |
| Planificarea pentru VPN | 35 | Erorile obișnuite de configurare VPN și cum se pot repara | 56 |
| Cerințele pentru setarea VPN | 35 | Depanarea VPN cu jurnalul QIPFILTER | 61 |
| Determinarea tipului de VPN ce urmează să fie creat | 36 | Depanarea VPN cu jurnalul QVPN | 63 |
| Completarea foilor de lucru pentru planificarea VPN-ului | 37 | Depanarea VPN cu istoricul de job VPN | 65 |
| Configurarea VPN-ului | 40 | Depanarea VPN cu urmărirea comunicațiilor | 71 |
| Ce tip de conexiune ar trebui să configurez? | 40 | Informații înrudite pentru VPN | 73 |
| Cum configurez o conexiune dinamică VPN?. | 41 | Anexa. Observații | 75 |
| Cum configurez o conexiune VPN manual? | 42 | Mărci comerciale | 77 |
| Configurarea conexiunilor VPN cu vrăjitorul Conexiune nouă | 42 | Termenii și condițiile | 77 |
| Configurați politicile de securitate VPN | 43 | | |
| Configurarea conexiunilor sigure VPN. | 44 | | |

VPN (Virtual Private Networking)

O rețea privată virtuală (VPN - virtual private network) permite companiei dumneavoastră să își extindă în siguranță intranetul propriu în cadrul unei rețele publice, cum este Internet. Cu VPN, compania dumneavoastră poate controla traficul de rețea și furniza caracteristici importante de securitate, cum ar fi autentificarea și confidențialitatea datelor.

VPN este o componentă care poate fi instalată opțional din Navigator iSeries, interfața grafică cu utilizatorul (GUI) pentru i5/OS. Ea vă permite să creați o cale sigură capăt-la-capăt pentru orice combinație de gazdă și gateway. VPN folosește metode de autentificare, algoritmi de criptare și alte măsuri de precauție pentru ca datele trimise între cele două puncte ale conexiunii să rămână sigure.

VPN rulează la nivelul de rețea ale stivei de protocoale TCP/IP. Mai precis, VPN folosește cadrul de lucru deschis IPSec (IP Security Architecture). IPSec furnizează funcții primare de securitate pentru Internet, precum și elemente flexibile cu care puteți crea rețele private virtuale robuste și sigure.

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

Este important să înțelegeți efectul pe care îl va avea VPN asupra întregii dumneavoastră rețele. Planificarea și implementarea corectă sunt esențiale pentru succesul dumneavoastră. Revedeți aceste subiecte pentru a vă asigura că știți cum funcționează VPN-urile și cum ați putea să le folosiți:

Ce este nou pentru V5R4

Prezintă informațiile noi sau modificate semnificativ în această ediție.

Funcție nouă: TFC (Traffic Flow Confidentiality)

TFC (Traffic Flow Confidentiality) vă permite să ascundeți lungimea reală a pachetelor de date transferate peste o conexiune VPN. Folosiți TFC pentru o securitate suplimentară împotriva atacatorilor care ar putea ghici tipul de date care se trimit peste conexiunea VPN din lungimea pachetului de date. Puteți folosi TFC doar dacă politica de date este setată pentru modul Tunel.

- “Configurarea TFC (Traffic Flow Confidentiality)” la pagina 51

Funcție nouă: ESN (Extended Sequence Number)

ESN vă permite să transmiteți volume mari de date la o viteză mare fără să fie necesară să faceți frecvent retransmiterea cheilor. Puteți activa ESN doar când politica de date folosește protocolul AH (Authentication Header) sau protocolul ESP (Encapsulation Security Payload) și AES ca algoritm de criptare.

- “Configurarea ESN (Extended Sequence Number)” la pagina 51



Scenariu nou: VPN prietenos pentru firewall

În acest scenariu aflați cum să stabiliți o conexiune VPN unde gateway-ul (client) și gazda (server) sunt în spatele unui firewall care rulează NAT (Network Address Translation).

- “Scenariu: VPN prietenos pentru firewall” la pagina 28

Cum puteți vedea ce este nou sau modificat


Pentru a vă ajuta să vedeți ce modificări tehnice au fost făcute, aceste informații folosesc:

- Imaginea  pentru a marca unde încep informații noi sau modificate.
- Imaginea  pentru a marca unde se termină informațiile noi sau modificate.

Pentru a afla alte informații despre ce este nou sau modificat la această ediție, vedeți Memo către utilizatori.

PDF tipăribil

Folosiți aceasta pentru a vizualiza sau pentru a tipări un PDF cu aceste informații.

Pentru a vedea sau descărca versiunea PDF a acestui document, selectați VPN (Virtual private networking)  (în jur de 509 KB).

Salvarea fișierelor PDF

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

1. Faceți clic dreapta pe PDF în browser (faceți clic dreapta pe legătura de mai sus).
2. Faceți clic pe **Save Target As...** dacă folosiți Internet Explorer. Faceți clic pe **Save Link As** dacă folosiți Netscape Communicator.
3. Navigați la directorul în care doriți să salvați fișierul PDF.
4. Faceți clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

Aveți nevoie de Acrobat Reader pentru a vedea sau tipări aceste PDF-uri. Puteți descărca o copie de pe site-ul Web Adobe (www.adobe.com/products/acrobat/readstep.html) .

Conceptele VPN

Este important să aveți cel puțin cunoștințe de bază în ceea ce privește tehnologiile VPN standard. Acest subiect vă furnizează informații conceptuale despre protocoalele folosite de VPN.

Rețeaua privată virtuală (VPN) folosește mai multe protocoale TCP/IP importante pentru a proteja traficul de date. Pentru a înțelege mai bine cum funcționează o conexiune VPN, familiarizați-vă cu aceste protocoale și concepte și cu felul în care le folosește VPN:

Protocoalele IP Security (IPSec)

IPSec oferă o bază stabilă și durabilă pentru furnizarea de securitate la nivelul rețea.

IPSec suportă toți algoritmi de criptare folosiți în prezent și poate de asemenea îngloba algoritmi noi și mai puternici pe măsură ce aceștia apar. Protocoalele IPSec tratează aceste probleme majore de securitate:

Autentificarea originii datelor

Verifică dacă fiecare datagramă a fost lansată de emițătorul declarat.

Integritatea datelor

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

Confidențialitatea datelor

Ascunde conținutul unui mesaj, de obicei prin criptare.

Protecția la redare

Asigurați că un atacator nu poate intercepta o datagramă pentru a o reda ulterior.

Gestionarea automată a cheilor criptografice și a asociațiilor de securitate

Asigurați-vă că politica dumneavoastră VPN poate fi utilizată prin rețeaua extinsă cu o configurație manuală redusă sau chiar fără.

VPN folosește două protocoale IPSec pentru a proteja datele care trec prin VPN: Authentication Header (AH) și 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) și generarea și reînnoșirea automată a cheilor de securitate.

Notă: Unele configurații VPN pot avea un punct vulnerabil din punct de vedere securitate, în funcție de cum este configurat IPSec. Vulnerabilitatea afectează configurațiile unde IPSec este configurat să folosească ESP (Encapsulating Security Payload) în modul tunel cu confidențialitate (criptare), dar fără protecție de integritate (autentificare) sau AH (Authentication Header). Configurația implicită când este selectat ESP include întotdeauna un algoritm de autentificare care oferă protecția la integritate. De aceea, doar dacă algoritmul de autentificare nu este înlăturat din transformarea ESP, configurațiile VPN vor fi protejate împotriva acestei vulnerabilități. Configurația VPN IBM Universal Connection nu este afectată de această vulnerabilitate.

Pentru a verifica dacă sistemul este afectat de această vulnerabilitate de securitate, urmați acești pași:

1. În Navigator iSeries, expandați serverul > **Rețea** → **Politici IP** → **VPN** → **Politici de securitate IP** → **Politici de date**.
2. Faceți clic dreapta pe politica de date pe care vreți să o verificați și selectați **Proprietăți**.
3. Faceți clic pe fișa **Propuneri**.
4. Selectați orice propunere de protecție de date care folosește protocolul ESP și faceți clic pe **Editare**.
5. Faceți clic pe fișa **Transformări**.
6. Selectați orice transformare din listă care folosește protocolul ESP și faceți clic pe **Editare**.
7. Verificați că algoritmul de autentificare are orice altă valoare decât **Fără**.

Internet Engineering Task Force (IETF) definește formal IPSec în RFC 2401, *Security Architecture for the Internet Protocol*. Puteți vedea acest RFC pe Internet la următoarea adresă Web: <http://www.rfc-editor.org>.

Principalele protocoale IPSec sunt listate mai jos:

Concepte înrudite

“Gestionarea cheilor” la pagina 6

Un VPN dinamic furnizează securitate suplimentară pentru comunicațiile 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.

Informații înrudite

<http://www.rfc-editor.org>

Authentication Header

Protocolul Authentication Header (AH) furnizează autentificarea originii datelor, integritatea datelor și protecție la redare. Totuși, AH nu oferă confidențialitatea 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 folosește pentru autentificare. Pentru a asigura protecția la redare, AH folosește un câmp de numere de ordine din cadrul antetului AH. Trebuie menționat că aceste trei funcții diferite sunt deseori grupate și numite **autentificare**. În cei mai simpli termeni, AH asigură că nu s-a umblat la datele dumneavoastră pe drumul lor până la destinația finală.

Deși 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**. Totuși, AH întotdeauna protejează conținutul pachetului IP.

Internet Engineering Task Force (IETF) definește formal AH în Request for Comment (RFC) 2402, *IP Authentication Header*. Puteți vedea acest RFC pe Internet la următoarea adresă Web: <http://www.rfc-editor.org>.

Moduri de folosire a AH

Puteți aplica AH în două moduri: modul transport sau modul tunel. În modul transport, antetul IP al datagramii este cel mai exterior antet IP, urmat de antetul AH și apoi de conținutul datagramii. AH autentifică întreaga datagramă, cu excepția câmpurilor variabile. Totuși, informațiile conținute în datagramă sunt transportate transparent și pot fi, astfel, spionate. Modul transport necesită mai puțină procesare suplimentară decât modul tunel, dar nu oferă la fel de multă securitate.

Modul tunel creează un nou antet IP și îl folosește drept cel mai exterior antet IP al datagramii. Antetul AH urmează noul antet IP. Datagrama originală (antetul IP și conținutul 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, folosiți modul tunel. În modul tunel adresele sursă și destinație din cel mai exterior antet IP nu trebuie să fie la fel ca acelea din antetul IP original. De exemplu, două porți de securitate pot funcționa cu un tunel AH pentru a autentifica tot traficul dintre rețelele 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 folosiți 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 performanțele sistemului dumneavoastră așa cum face ESP. Alt avantaj al folosirii AH, este că AH autentifică întreaga datagramă. ESP, totuși, nu autentifică antetul IP din frunte sau orice alte informații care apar înainte de antetul ESP.

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

Folosirea ESN cu AH

- | Dacă folosiți protocolul AH atunci puteți dori să activați ESN (Extended Sequence Number). ESN vă permite să
- | transmiteți volume mari de date la o viteză mare fără să fie necesară retransmiterea cheilor (re-keying). Conexiunea
- | VPN folosește numere de ordine pe 64 de biți în locul numerelor pe 32 de biți peste IPSec. Folosind numere de ordine
- | de 64 de biți permite mai mult timp înainte de retransmiterea cheilor, care împiedică epuizarea și minimizarea folosirii
- | resurselor de sistem.

Ce algoritmi folosește AH pentru a-mi proteja informațiile?

AH folosește algoritmi cunoscuți drept **HMAC (hashed message authentication codes)**. În mod specific, VPN folosește fie HMAC-MD5 fie HMAC-SHA. Atât MD5, cât și SHA folosesc date de intrare de lungime variabilă și o cheie secretă pentru a produce date de ieșire de lungime fixă (numită valoare hash). Dacă valorile hash ale unor mesaje coincid, este foarte probabil ca mesajele să fie identice. Atât MD5, cât și SHA criptează lungimea mesajului la ieșire, dar SHA este considerat mai sigur deoarece produce hash-uri mai mari.

Internet Engineering Task Force (IETF) definește formal HMAC-MD5 în RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Internet Engineering Task Force (IETF) definește formal HMAC-SHA în RFC 2404, *The Use*

of HMAC-SHA-1-96 within ESP and AH. Puteți vedea aceste RFC-uri pe Internet la următoarea adresă Web: <http://www.rfc-editor.org>.

Concepte înrudite

“Encapsulating Security Payload”

Protocolul Encapsulating Security Payload (ESP) furnizează confidențialitatea datelor și, opțional, autentificarea originii datelor, verificarea integrității datelor și protecție la redare.

Informații înrudite

<http://www.rfc-editor.org>

Encapsulating Security Payload

Protocolul Encapsulating Security Payload (ESP) furnizează confidențialitatea datelor și, opțional, autentificarea originii datelor, verificarea integrității datelor și protecție la redare.

Diferența dintre ESP și protocolul Authentication Header (AH) constă în faptul că ESP furnizează criptare, în timp de ambele protocole furnizează autentificare, verificare de integritate și protecție la redare. Cu ESP, ambele sisteme care comunică folosesc o cheie partajată pentru criptarea și decriptarea datelor schimbate.

Dacă vă decideți să folosiți atât criptare, cât și autentificare, sistemul care răspunde mai întâi autentifică pachetul și apoi, dacă primul pas reușește, sistemul continuă cu decriptarea. Acest tip de configurație reduce procesarea suplimentară și vulnerabilitatea la atacuri prin negarea-serviciilor.

Două moduri de a folosi ESP

Puteți folosi ESP în două moduri: modul transport și modul tunel. În modul transport, antetul ESP urmează antetul IP al datagrammei IP originale. Dacă datagrama are deja un antet IPSec, atunci antetul ESP vine înaintea lui. Trailer-ul ESP și datele opționale de autentificare urmează după datele utile.

Modul transport nu autentifică sau criptează antetul IP, ceea ce ar putea expune informațiile dumneavoastră de adresă unor potențiali atacatori în timp ce datagrama este în tranzit. Modul transport necesită mai puțină 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 și îl folosește ca antet IP exterior al datagrammei, urmat de antetul ESP și apoi de datagrama originală (atât antetul IP, cât și datele utile originale). Trailer-ul ESP și datele opționale de autentificare sunt atașate la datele utile. Când folosiți atât criptare, cât și autentificare, ESP protejează complet datagrama originală deoarece aceasta reprezintă acum datele utile pentru noul pachet ESP. ESP nu protejează totuși noul antet IP. Gateway-urile trebuie să folosească ESP în modul tunel.

Ce algoritmi folosește ESP pentru a proteja informațiile?

ESP folosește o cheie simetrică, cu care ambele părți criptează și decriptează datele pe care le schimbă. Transmițătorul și receptorul trebuie să se înțeleagă asupra cheii înainte de a putea comunica în siguranță. VPN utilizează DES (Data Encryption Standard), 3DES (triplu-DES), RC5, RC4 și AES (Advanced Encryption Standard) pentru criptare.

- | Dacă alegeți algoritmul AES, atunci puteți dori să activați ESN (Extended Sequence Number). ESN vă permite să
- | transmiteți volume mari de date la o viteză mare. Conexiunea VPN folosește numere de ordine pe 64 de biți în locul
- | numerelor pe 32 de biți peste IPSec. Folosind numere de ordine de 64 de biți permite mai mult timp înainte de
- | retransmiterea cheilor, care împiedică epuizarea și minimizarea folosirii resurselor de sistem.

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

ESP folosește algoritmi HMAC-MD5 și HMAC-SHA pentru a furniza funcții de autentificare. Atât MD5, cât și SHA folosesc date de intrare de lungime variabilă și o cheie secretă pentru a produce date de ieșire de lungime fixă (numită

valoare hash). Dacă valorile hash ale unor mesaje coincid, este foarte probabil ca mesajele să fie identice. Atât MD5, cât și SHA criptează lungimea mesajului la ieșire, dar SHA este considerat mai sigur deoarece produce hash-uri mai mari.

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

Concepte înrudite

“Authentication Header” la pagina 3

Protocolul Authentication Header (AH) furnizează autentificarea originii datelor, integritatea datelor și protecție la redare. Totuși, AH nu oferă confidențialitatea datelor, ceea ce înseamnă că toate datele dumneavoastră sunt trimise transparent.

Informații înrudite

<http://www.rfc-editor.org>

AH și ESP combinate

VPN vă permite să combinați AH și ESP pentru conexiuni gazdă-la-gazdă în modul transport.

Combinarea acestor protocoale protejează întreaga datagramă IP. Deși combinarea celor două protocoale oferă mai multă securitate, procesarea suplimentară pe care o implică poate să depășească beneficiile.

Gestionarea cheilor

Un VPN dinamic furnizează securitate suplimentară pentru comunicațiile 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.

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

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

O **asociere de securitate (SA)** conține informații care sunt necesare pentru a folosi protocoale IPSec. De exemplu, o SA identifică tipurile de algoritmi, lungimile și duratele de viață ale cheilor, părțile participante și modulele de încapsulare.

Cheile criptografice, după cum implică și numele, blochează, sau protejează, informațiile dumneavoastră până când ajunge în siguranță la destinația ei finală.

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

Fazele gestionării cheilor

Managerul de chei VPN folosește două faze distincte în implementare.

Faza 1 Faza 1 stabilește o cheie secretă principală din care sunt derivate toate cheile criptografice următoare pentru a proteja traficul de date al utilizatorului. Acest lucru este adevărat chiar dacă încă nu există nici o protecție de securitate între cele două capete. VPN folosește ori modul semnătură RSA, ori chei prepartajate pentru a autentifica negocierile din faza 1, ca și pentru a stabili cheile care protejează mesajele IKE care circulă în timpul negocierilor din faza 2.

O *cheie prepartajată* este un șir de caractere neobișnuite, 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 poștă înregistrată, înaintea negocierilor IKE. Tratați cheia prepartajată ca pe o parolă.

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

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

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

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

Când creați un VPN dinamic utilizând Navigator iSeries, trebuie să definiți o politică IKE pentru a activa negocierile din faza 1 și o politică de date pentru a guverna negocierile din faza 2. În mod opțional, puteți folosi vrăjitorul de Conexiune nouă. Vrăjitorul creează automat fiecare dintre obiectele de configurare pe care le necesită VPN pentru a funcționa corect, inclusiv o politică IKE și o politică de date.

Lecturi recomandate

Dacă vreți să citiți mai multe despre protocolul IKE (Internet Key Exchange) și despre gestiunea cheie, revedeți 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)*

Puteți vedea aceste RFC-uri pe Internet la următoarea adresă Web: <http://www.rfc-editor.org>.

Concepte înrudite

“Scenariu: VPN prietenos pentru firewall” la pagina 28

În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago și o gazdă din Minneapolis, atunci când amândouă serverele sunt în spatele unui firewall.

“Protocoalele IP Security (IPSec)” la pagina 2

IPSec oferă o bază stabilă și durabilă pentru furnizarea de securitate la nivelul rețea.

Operații înrudite

“Configurarea unei politici IKE (Internet Key Exchange)” la pagina 43

Politica IKE definește ce nivel de autentificare și protecție prin criptare folosește IKE în timpul fazei 1 a negocierilor.

“Configurarea unei politici de date” la pagina 44

O politică de date definește ce nivel de autentificare sau criptare protejează datele care circulă prin VPN.

Informații înrudite

Layer 2 Tunnel Protocol (L2TP)

Folosiți aceste informații pentru a afla despre crearea unei conexiuni VPN pentru a securiza comunicațiile între rețeaua dumneavoastră și clienții de la distanță.

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

L2TP suportă două feluri de tunel: tunelul voluntar și tunelul obligatoriu. Diferența majoră dintre aceste două moduri de tunel este punctul final. La tunelul voluntar, tunelul se termină la clientul la distanță, pe când tunelul obligatoriu se termină la ISP.

Cu un **tunel obligatoriu** L2TP, o gazdă la distanță inițiază o conexiune cu Furnizorul său de Servicii Internet (ISP). Apoi ISP-ul stabilește o conexiune L2TP între utilizatorul la distanță și rețeaua companiei. Deși ISP stabilește conexiunea, dumneavoastră decideți cum să protejați traficul folosind VPN. Pentru un tunel obligatoriu, ISP-ul trebuie să suporte L2TP.

Cu un **tunel voluntar** L2TP, conexiunea este creată de utilizatorul la distanță, de obicei folosind un client de tunel L2TP. Astfel, utilizatorul trimite pachete L2TP către ISP-ul său, care le înaintează către rețeaua 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 configurați un sistem dintr-un birou de filială să se conecteze la rețeaua sa corporativă printr-un sistem gateway cu un tunel L2TP protejat de VPN.

Puteți vedea o prezentare vizuală despre conceptul de tuneluri voluntare L2TP protejate de IPSec. Aceasta necesită Flash plug-in. Alternativ, puteți folosi versiunea HTML a acestei prezentări.

L2TP este de fapt o variație 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 și destinație ale acestui pachet definesc punctele finale ale conexiunii. Deoarece protocolul de încapsulare exterioară este IP, puteți aplica protocoale IPSec la pachetul IP compus. Aceasta protejează datele care circulă în tunelul L2TP. Puteți aplica apoi protocoalele AH, ESP și IKE în mod direct.

Concepte înrudite

“Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec” la pagina 22

În acest scenariu, aflați cum să setați o conexiune între o gazdă a filialei și sediul central care folosește L2TP protejat de IPSec. Biroul filialei are o adresă IP alocată dinamic, în timp ce biroul companiei are o adresă IP statică, rutabilă global.

Text Flash VPN L2TP

O rețea privată virtuală (VPN - virtual private network) permite companiei dumneavoastră să își extindă în siguranță intranetul propriu în cadrul unei rețele publice, cum este Internet. VPN suportă L2TP (Layer 2 Tunnel Protocol). Soluțiile L2TP furnizează utilizatorilor la distanță acces sigur, cu cost redus la rețeaua corporativă. Prin stabilirea unui tunel către serverul rețea L2TP (LNS), clientul la distanță devine de fapt o extensie a rețelei corporative.

Acest scenariu conceptual afișează un sistem client la distanță care se conectează la rețeaua sa corporativă prin crearea unui tunel voluntar L2TP protejat de VPN.

Pentru a începe, clientul la distanță stabilește o conexiune la Internet prin intermediul ISP (Internet Service Provider). ISP-ul atribuie clientului o adresă IP rutabilă global.

Necunoscut ISP-ului, clientul inițiază o conexiune VPN cu gateway-ul VPN corporativ. Gateway-ul autentifică sistemul client care vrea să acceseze rețeaua corporativă.

După ce clientul primește autentificarea de la gateway (făcând conexiunea sigură), acesta stabilește tunelul L2TP. Clientul utilizează încă adresa IP atribuită de ISP. Tunelul L2TP va permite în final datelor să circule între sistemul client și gateway-ul colectiv.

O dată ce tunelul L2TP (afișat în galben) este stabilit, LNS atribuie clientului o adresă IP din schema de adrese a rețelei corporative. Nu există nici o linie fizică asociată conexiunii, așa că este creată o linie virtuală pentru a permite traficului PPP să circule prin tunelul L2TP.

Acum traficul IP poate circula între sistemul client la distanță și orice sistem din rețeaua corporativă.

Translatarea adreselor de rețea pentru VPN

VPN furnizează un mijloc pentru efectuarea de translatare a adreselor de rețea, denumit VPN NAT. VPN NAT diferă de NAT tradițional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE și IPSec. Studiați acest subiect pentru a afla mai multe.

Translatarea adreselor de rețea (Network address translation - NAT) ia adresele IP private și le translatează în adrese publice IP. Aceasta ajută la economisirea valoroaselor adrese publice, permițând în același timp calculatoarelor gazdă din rețeaua dumneavoastră să acceseze servicii și gazde la distanță de pe Internet (sau din alte rețele publice).

În plus, dacă folosiți adrese IP private, acestea pot intra în coliziune cu adrese IP de intrare similare. De exemplu, ați putea dori să comunicați cu altă rețea dar ambele rețele folosesc adrese 10.*.*., provocând coliziunea adreselor și pierderea tuturor pachetelor. Aplicarea NAT asupra adreselor de ieșire ar putea părea răspunsul la această problemă. Oricum, dacă traficul de date este protejat de un VPN, translatarea NAT convențională nu va funcționa deoarece modifică adresele IP din asocierile de securitate (security associations - SAs) pe care le necesită VPN pentru a funcționa. Pentru a evita această problemă, VPN oferă propria versiune de translatare a adreselor de rețea 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 ștergeți 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 luați în considerare înainte să începeți. Acestea sunt:

VPN NAT pentru prevenirea conflictelor între adresele IP

Acest tip de VPN NAT vă permite să evitați posibile conflicte între adrese IP când configurați o conexiune VPN între rețele 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 configurați acest tip de VPN NAT depinde de faptul că serverul dumneavoastră este inițiatorul conexiunii VPN sau respondent. Când serverul dumneavoastră este inițiatorul conexiunii, puteți transla 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, puteți transla adresele la distanță ale partenerului dumneavoastră de VPN în unele care sunt compatibile cu schema dumneavoastră locală de adresare. Configurați 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 faceți disponibilă public. Când configurați VPN NAT, puteți decide ca fiecare adresă IP cunoscută public să fie translatată într-una dintr-un set de adrese ascunse. Aceasta vă permite de asemenea să echilibrați încărcarea traficului pentru o adresă individuală prin repartizarea mai multor adrese. VPN NAT pentru adrese locale necesită ca serverul dumneavoastră să acționeze ca respondent la conexiuni.

Folosiți VPN NAT pentru ascunderea adreselor locale dacă răspundeți da la aceste întrebări:

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

Scenariul, Utilizare translatare adresă rețea pentru VPN vă furnizează un exemplu de cum să configurați VPN NAT să ascundă adresele locale din iSeries.

Pentru instrucțiuni pas-cu-pas despre cum să setați VPN NAT pe sistemul dumneavoastră, folosiți ajutorul online disponibil în interfața VPN din Navigator iSeries.

Concepte înrudite

“Scenariu: Folosirea translatării adreselor de rețea pentru VPN” la pagina 33

În acest scenariu, compania dumneavoastră vrea să schimbe date confidențiale cu unul dintre partenerii ei de afaceri utilizând VPN. Pentru a proteja și mai mult structura rețelei, compania dumneavoastră va folosi de asemenea VPN NAT, pentru a ascunde adresa IP privată a sistemului pe care îl folosește pentru a găzdui aplicațiile la care are acces partenerul de afaceri.

“Foaia de lucru pentru planificarea conexiunilor” la pagina 38

Completați această foaie de lucru înainte de a vă configura o conexiune manuală.

IPSec compatibil NAT cu UDP

Încapsularea UDP permite traficului IPSec să treacă printr-un dispozitiv NAT convențional. Treceți în revistă acest subiect pentru mai multe informații despre ce este și de ce ar trebui să îl folosiți pentru conexiunile dumneavoastră VPN.

Problema: NAT-ul convențional întrerupe VPN-ul

Translatarea adreselor de rețea (NAT) vă permite să ascundeți adresele IP private neînregistrate în spatele unui set de adrese IP înregistrate. Aceasta vă ajută să vă protejați rețeaua internă de rețelele 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 convențional nu funcționează 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 și negocierile conexiunii VPN eșuează.

Soluția: Încapsularea UDP

Într-un înveliș, 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 destinație, capătul receptor înlătură antetul suplimentar, lăsând pachetul IPSec original, care va trece acum toate celelalte validări.

Puteți să aplicați încapsularea UDP doar la VPN-uri care vor folosi IPSec ESP în modul tunel sau modul transport. În plus, la V5R2 serverul iSeries se poate comporta doar ca un client pentru încapsularea UDP. Cu alte cuvinte, poate doar să inițieze trafic încapsulat UDP.

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

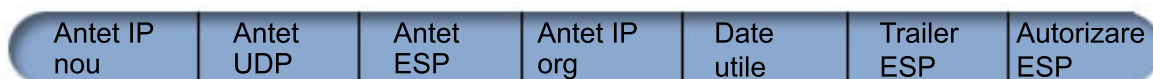
Datagrama IPv4 originală:



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. Totuși, când IKE detectează NAT în timpul negocierii cheie, pachetele IKE următoare sunt trimise prin portul sursă 4500, portul destinație 4500. Aceasta înseamnă de asemenea că portul 4500 trebuie să nu fie restricționat în nici o regulă filtru aplicabilă. Capătul receptor al conexiunii poate determina dacă pachetul este unul IKE sau unul încapsulat UDP deoarece primii 4 octeți ai datelor utile UDP sunt setați pe zero pe un pachet IKE. Pentru a funcționa corect, ambele capete ale conexiunii trebuie să suporte încapsularea UDP.

Concepte înrudite

“Scenariu: VPN prietenos pentru firewall” la pagina 28

În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago și o gazdă din Minneapolis, atunci când amândouă serverele sunt în spatele unui firewall.

Comprimarea IP (IPComp)

IPComp reduce dimensiunea datagramelor IP prin comprimarea datagramelor pentru a crește performanțele comunicațiilor dintre doi parteneri VPN.

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

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

Informații înrudite

<http://www.rfc-editor.org>

VPN și filtrarea IP

Filtrarea IP și VPN sunt foarte înrudite. De fapt, majoritatea conexiunilor VPN necesită reguli de filtrare pentru a funcționa corect. Acest subiect vă oferă informații despre ce filtre necesită VPN, împreună cu alte concepte de filtrare înrudite cu VPN.

Cele mai multe conexiuni VPN necesită reguli filtru pentru a funcționa corect. Regulile de filtrare necesare depind de tipul de conexiune VPN pe care o configurați, ca și de tipul de trafic pe care doriți să-l controlați. În general, fiecare conexiune va avea un filtru de politică. Filtrul de politică definește care adrese, protocoale și 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 ediția OS/400 V5R1, VPN poate genera aceste reguli în mod automat. Când este posibil, permiteți VPN-ului să genereze filtrele de politică pentru dumneavoastră. Aceasta nu va ajuta doar la eliminarea erorilor, dar elimină de asemenea și nevoia ca dumneavoastră să configurați regulile ca un pas separat, folosind editorul Reguli pachet din Navigator iSeries.

Desigur, sunt și excepții. Treceți în revistă aceste subiecte pentru a afla mai multe despre alte concepte și tehnici de filtrare VPN, mai puțin obișnuite, care pot fi valabile în cazul dumneavoastră:

Concepte înrudite

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Conexiuni VPN fără filtre de politici

În cazul în care punctele finale ale conexiunii dumneavoastră VPN sunt adrese IP specifice, singulare și doriți să porniți VPN fără a fi nevoie să scrieți sau să activați reguli de filtrare pe sistem, puteți configura un filtru de politică dinamic. Acest subiect explică de ce ați putea lua în considerare acest lucru și vă descrie cum să îl faceți.

O regulă de filtrare politică definește care adrese, protocoale și porturi pot utiliza un VPN și dirijează traficul corespunzător prin conexiune. În unele cazuri, ați putea dori să configurați o conexiune care nu necesită o regulă de filtrare politici. De exemplu, puteți avea reguli pentru pachete non-VPN încărcate în interfața pe care o va folosi conexiunea dumneavoastră VPN, astfel că, în loc să dezactivați regulile active de pe acea interfață, vă decideți să configurați 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 puteți folosi un filtru dinamic de politici pentru conexiunea dumneavoastră VPN, trebuie să fie adevărate următoarele:

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

Dacă toate aceste condiții sunt îndeplinite de conexiunea dumneavoastră, o puteți 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 instrucțiuni pas-cu-pas despre cum să configurați o conexiune astfel încât să nu necesite un filtru politică, utilizați ajutorul online pentru VPN.

IKE Implicit

Pentru a se realiza negocieri IKE pentru VPN-ul dumneavoastră, trebuie să permiteți 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.

Pentru a stabili o conexiune, cele mai multe VPN-uri necesită apariția unor negocieri IKE (Internet Key Exchange) înainte de procesarea IPSec. IKE folosește binecunoscutul port 500, astfel că pentru ca IKE să funcționeze bine, trebuie

să permiteți 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. Totuși, regulile scrise specific pentru traficul portului 500 UDP sunt tratate pe baza a ceea ce e definit în regulile filtru active.

Scenarii VPN

Revedeți aceste scenarii pentru a vă familiariza cu detaliile tehnice și de configurare pe care le implică aceste tipuri de conexiune de bază.

Concepte înrudite

Scenariu QoS: Rezultate sigure și predictibile (VPN și QoS)

Informații înrudite

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

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

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

Scenariu: Conexiunea de bază cu biroul filialei

În acest scenariu, compania dumneavoastră vrea să stabilească un VPN între subrețelele a două departamente la distanță, printr-o pereche de calculatoare iSeries acționând ca gateway-uri VPN.

Situație

Să considerăm cazul în care compania dumneavoastră dorește minimizarea costurilor rezultate din comunicarea cu și între propriile filiale. În prezent, compania dumneavoastră folosește frame relay sau linii închiriate, dar vreți să luați explorări și alte opțiuni de transmitere a datelor confidențiale interne, care sunt mai puțin costisitoare, mai sigure și accesibile global. Prin exploatarea Internetului, puteți realiza ușor o rețea privată virtuală (VPN) pentru a îndeplini necesitățile companiei dumneavoastră.

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

Important: Acest scenariu arată gateway-urile de securitate iSeries atașate direct la Internet. Absența unui firewall are intenția de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luați în considerare riscurile de securitate implicate de fiecare dată când vă conectați la Internet.

Avantaje

Acest scenariu are următoarele avantaje:

- Folosirea Internetului sau a unui intranet existent reduce costul liniilor private între subrețele la distanță.
- Folosirea Internetului sau a unui intranet existent reduce complexitatea instalării și întreținerii liniilor private și a echipamentului asociat.
- Folosirea Internetului permite locațiilor la distanță să se conecteze aproape oriunde în lume.
- Folosirea VPN-ului furnizează utilizatorilor acces la toate serverele și resursele de pe fiecare parte a conexiunii, ca și când ar fi conectați folosind o linie închiriată sau o conexiune de tip rețea de arie întinsă (WAN).
- Folosirea metodelor standard de autentificare și de criptare asigură securitatea informațiilor sensibile, trimise de la o locație la alta.

- Schimbându-vă cheile de criptare dinamic și în mod regulat, se simplifică instalarea și se minimizează riscul decodificării cheilor și străpungerea securității.
- Utilizarea adreselor IP în fiecare subrețea la distanță face necesară alocarea adreselor IP publice pentru fiecare client.

Obiective

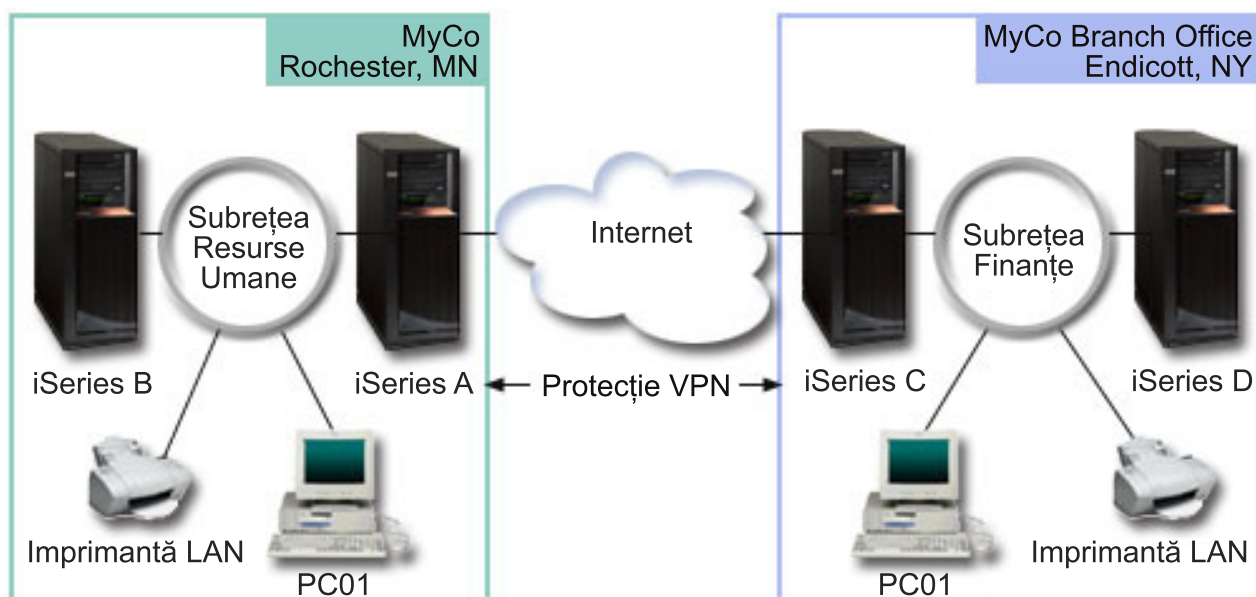
În acest scenariu, MyCo, Inc. vrea să stabilească un VPN între subrețelele departamentelor proprii de Resurse Umane și Finanțe, printr-o pereche de servere iSeries. Cele două servere se vor comporta ca gateway-uri VPN. Într-o configurație VPN, un gateway gestionează cheile și aplică IPSec datelor care 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 subrețeaua departamentului Resurse Umane și cea a departamentului Finanțe.
- Traficul de date nu necesită protecția VPN-ului după ce ajunge la una dintre subrețelele departamentelor.
- Toți clienții și gazdele din fiecare rețea au acces total la rețeaua celuilalt, inclusiv toate aplicațiile.
- Serverele gateway pot comunica între ele și își pot accesa aplicațiile între ele.

Detalii

Următoarea ilustrație prezintă caracteristicile rețelei MyCo.



Departamentul Resurse Umane

- Pe iSeries-A rulează OS/400 versiunea 5 ediția 2 (V5R2) și el se comportă ca un gateway VPN al Departamentului Resurse Umane.
- Subrețeaua este 10.6.0.0 cu masca 255.255.0.0. Această subrețea 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 și aplică IPSec datagramelor IP care vin și pleacă.
- iSeries-A se conectează la propriile subrețele cu adresa IP 10.6.11.1.
- iSeries-B este un server de producție din subrețeaua Resurse Umane, care rulează aplicații TCP/IP standard.

Departamentul Finanțe

- Pe iSeries-C rulează OS/400 versiunea 5 ediția 2 (V5R2) și el se comportă ca un gateway VPN al Departamentului Finanțe.
- Subrețeaua este 10.196.8.0 cu masca 255.255.255.0. Această subrețea 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 și aplică IPSec datagramelor IP care vin și pleacă.
- iSeries-C se conectează la propriile subrețele cu adresa IP 10.196.8.5.

Task-urile de configurare

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

Notă: Înainte de a porni aceste task-uri, verificați rutarea TCP/IP, pentru a vedea dacă cele două servere gateway pot comunica între ele prin Internet. În acest fel, vă asigurați că gazdele din fiecare subrețea rutează corespunzător către gateway-ul corespunzător pentru a accesa subrețeaua la distanță.

Concepte înrudite

Rutarea TCP/IP și echilibrarea încărcării

Informații înrudite

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

Completarea foilor de lucru pentru planificare

Următoarele liste de verificări pentru planificare arată tipul de informații de care aveți nevoie înainte de a începe configurarea VPN. Toate răspunsurile din lista de verificare a cerinței 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.

Tabela 1. Cerințe sistem

| Listă de verificare pentru cerințele preliminare | Răspunsuri |
|--|------------|
| Sistemul dumneavoastră de operare este OS/400 V5R2 (5722-SS1) sau ulterior? | Da |
| Este instalat Digital Certificate Manager (5722-SS1 opțiunea 34)? | Da |
| Este instalat iSeries Access pentru Windows (5722-XE1)? | Da |
| Este instalat Navigator iSeries? | Da |
| Este instalată subcomponenta Rețea din Navigator iSeries? | Da |
| Este instalat TCP/IP Connectivity Utilities (5722-TC1)? | Da |
| Ați setat la 1 valoarea de sistem pentru reținerea datelor de securitate ale serverului (QRETSVRSEC *SEC)? | Da |
| Este configurat TCP/IP pe sistem (inclusiv interfețele IP, rutele, numele de gazdă locală și numele de domeniu local)? | Da |
| Este stabilită comunicația TCP/IP normală între punctele finale cerute? | Da |
| Ați aplicat cele mai recente corecții 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 și ESP? | Da |
| Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH și ESP? | Da |
| Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP? | Da |

Tabela 2. Configurație VPN

| Aveți nevoie de aceste informații pentru a configura VPN-ul | Răspunsuri |
|--|--|
| Ce tip de conexiune creați ? | gateway-la-gateway |
| Cum veți denumi grupul de chei dinamice? | HRgw2FINGw |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? | echilibrate |
| Folosiți certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată? | Nu este topsecretstuff |
| Care este identificatorul serverului de chei local? | Adresa IP: 204.146.18.227 |
| Care este identificatorul punctului final de date local ? | Subrețea: 10.6.0.0 Mască: 255.255.0.0 |
| Care este identificatorul serverului de chei la distanță ? | Adresa IP: 208.222.150.250 |
| Care este identificatorul punctului final de date la distanță ? | Subrețea: 10.196.8.0 Mască: 255.255.255.0 |
| Ce porturi și protocoale doriți să permiteți prin conexiune ? | Oricare |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja datele? | echilibrate |
| Pe care dintre interfețe se aplică această conexiune ? | TRLINE |

Configurarea VPN-ului pe iSeries-A

Folosiți pași următori și informațiile din foile dumneavoastră de lucru pentru a configura VPN-ul pe iSeries-A:

1. În Navigator iSeries, expandați **iSeries-A** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Rețea privată virtuală** și selectați **Conexiune nouă** pentru a porni vrăjitorul Conexiune nouă.
3. Revedeți pagina **Bine ați venit** pentru informații despre ce obiecte creează vrăjitorul.
4. Faceți clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceți HRgw2FINGw.
6. Opțional: Specificați o descriere pentru acest grup de conexiuni.
7. Faceți clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectați **Conectarea gateway-ului dumneavoastră la alt gateway**.
9. Faceți clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.
11. Apăsați pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectați **Nu** pentru a indica faptul că nu veți folosi certificate pentru autentificarea conexiunii.
13. Apăsați **Următor** pentru a merge la pagina **Server de chei local**.
14. Selectați **Adresă IP Versiunea 4** din câmpul **Tip identificator**.
15. Selectați 204.146.18.227 din câmpul **Adresă IP**.
16. Apăsați **Următor** pentru a merge la pagina **Server de chei la distanță**.
17. Selectați **Adresa IP Versiunea 4** din câmpul **Tip de identificator**.
18. Introduceți 208.222.150.250 în câmpul **Identificator**.
19. Introduceți topsecretstuff în câmpul **Cheie prepartajată**.
20. Apăsați **Următor** pentru a merge la pagina **Punct final local de date**.
21. Selectați **Subrețea IP versiunea 4** din câmpul **Tip identificator**.
22. Introduceți 10.6.0.0 în câmpul **Identificator**.

23. Introduceți 255.255.0.0 în câmpul **Mască subrețea**.
24. Apăsați **Următor** pentru a merge la pagina **Punct final de date distanță**.
25. Selectați **Subrețea IP versiunea 4** din câmpul **Tip identificator**.
26. Introduceți 10.196.8.0 în câmpul **Identificator**.
27. Introduceți 255.255.255.0 în câmpul **Mască subrețea**.
28. Apăsați **Următor** pentru a merge în pagina **Servicii de date**.
29. Acceptați valorile implicite și apoi apăsați **Următor** pentru a merge în pagina **Politică de date**.
30. Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.
31. Selectați **Folosirea algoritmului de criptare RC4**.
32. Apăsați **Următor** pentru a merge la pagina **Interfețe aplicabile**.
33. Selectați **TRLINE** din tabelul **Linie**.
34. Apăsați **Următor** pentru a merge la pagina **Sumar**. Revedeți obiectele pe care le va crea pentru a asigura corectitudinea lor.
35. Apăsați pe **Sfârșit** pentru a termina configurarea.
36. Când apare caseta de dialog **Activare filtre politică**, selectați **Da, activare filtre de politică generate**, apoi selectați **Permitere totală a celuilalt trafic**.
37. Apăsați **OK** pentru a încheia configurarea. Când veți fi întrebat, specificați că doriți să activați regulile pe alte interfețe.

Configurarea VPN-ului pe iSeries-C

Parcurgeți aceiași pași ca la configurarea VPN-ului pe iSeries-A, înlocuind adresele IP după cum e necesar. Folosiți ca ghid foile de lucru pentru planificare. După ce terminați de configurat gateway-ul VPN al departamentului Finanțe, 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 porniți serverele VPN, dacă nu sunt deja pornite.

Pornirea serverelor VPN

Parcurgeți pașii următori pentru a porni serverele VPN:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **VPN** și selectați **Pornire**.

Testarea conexiunii

După ce ați terminat de configurat ambele servere și ați pornit cu succes serverele VPN, testați conectivitatea pentru a vă asigura că subrețelele la distanță pot comunica una cu cealaltă. Pentru aceasta, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **iSeries-A** → **Rețea**.
2. Faceți clic dreapta pe **Configurarea TCP/IP** și selectați **Utilitare** și apoi selectați **Ping**.
3. Din caseta de dialog **Ping de la**, introduceți iSeries-C în câmpul **Ping**.
4. Faceți clic pe **Ping acum** pentru verificarea conectivității de la iSeries-A la iSeries-C.
5. Faceți clic pe **OK** când ați terminat.

Scenariu: Conexiunea de bază companie la companie

În acest scenariu, compania dumneavoastră vrea să stabilească un VPN între o stație de lucru client din divizia dumneavoastră de producție și o stație de lucru client din departamentul de aprovizionare al unui partener de afaceri.

Situație

Multe companii folosesc frame relay sau linii închiriate pentru comunicații sigure cu partenerii lor de afaceri, finanțatori și furnizori. Din păcate, aceste soluții sunt mai întotdeauna scumpe și limitate geografic. VPN oferă o soluție alternativă pentru companiile care vor comunicații private cu cost redus.

Se consideră situația în care sunteți un furnizor important de subansamble al unui producător. Pentru că este vital să aveți produsele specifice și cantitățile exact la timpul cerut de firma producătoare, trebuie să dispuneți mereu de starea inventarului producătorului și de programele de producție. Poate că în prezent realizați această interacțiune manual și constatați că este mare consumatoare de timp, implică un cost ridicat și uneori apar date eronate. Ca urmare, vreți să găsiți o cale mai ușoară, mai rapidă și mai eficientă pentru comunicarea cu compania producătorului. Având în vedere confidențialitatea acestor informații, producătorul nu dorește să le publice pe propriul sit Web sau să le distribuie lunar printr-un raport extern. Exploatând Internetul public, puteți stabili ușor o rețea privată virtuală (VPN), pentru a satisface nevoile ambelor companii.

Obiective

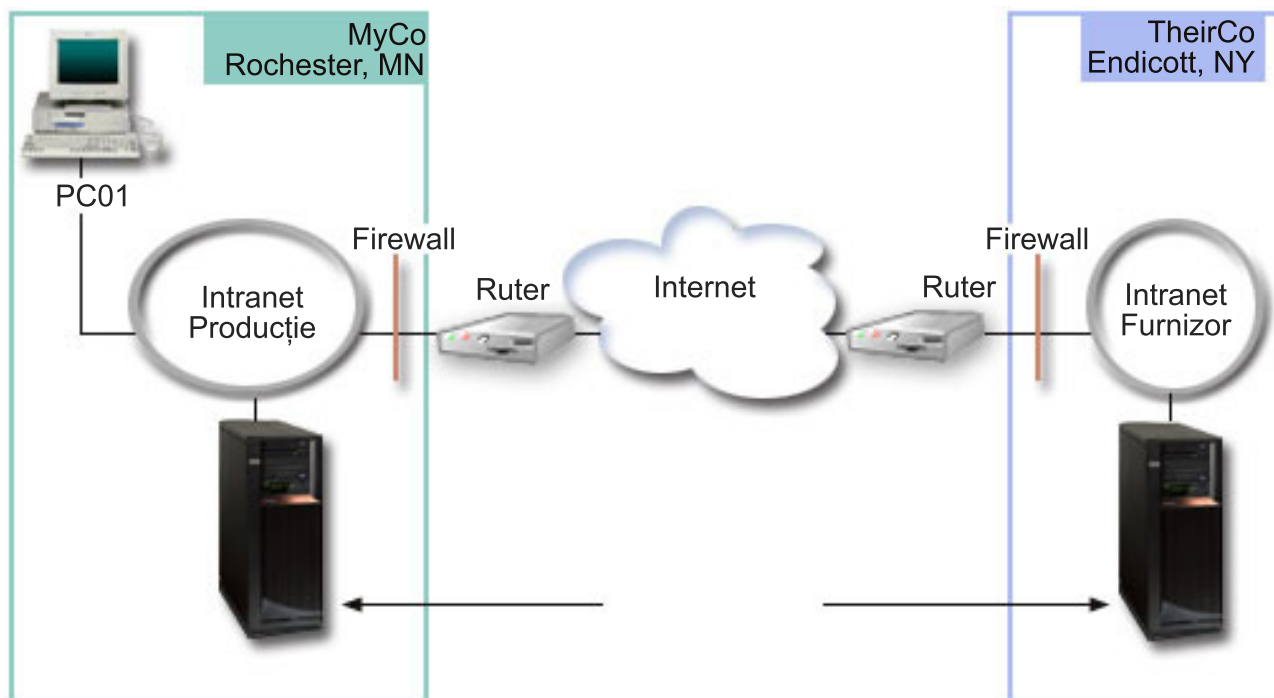
În acest scenariu, MyCo vrea să stabilească un VPN între o gazdă din divizia sa de subansamble și o gazdă din departamentul de producție al unuia dintre partenerii de afaceri, TheirCo.

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

Important: Intenția acestui scenariu este să facă o prezentare introductivă, prin exemplu, a unei configurații VPN simple gazdă-la-gazdă. Într-un mediu de rețea tipic, va trebuie să luați în considerare și configurarea unui firewall, cerințele de adresare IP și rutarea, printre altele.

Detalii

Următoarea ilustrație prezintă caracteristicile de rețea ale MyCo și TheirCo:



Rețeaua de aprovizionare MyCo

- Pe iSeries-A rulează OS/400 versiunea 5 ediția 2 (V5R2).
- iSeries-A are o adresă IP 10.6.1.1. Aceasta este punctul final al conexiunii, precum și punctul final de date. Aceasta pentru că iSeries-A realizează negocieri IKE și aplică IPSec datagramelor IP de intrare și ieșire și este de asemenea sursa și destinația pentru datele care circulă prin VPN.
- iSeries-A este în subrețeaua 10.6.0.0 cu masca 255.255.0.0
- Doar iSeries-A poate iniția conexiunea cu iSeries-C.

Rețeaua de producție a TheirCo

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

Task-urile de configurare

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

Notă: Înainte de a porni aceste task-uri, verificați rutarea TCP/IP, pentru a vedea dacă cele două servere gateway pot comunica între ele prin Internet. În acest fel, vă asigurați că gazdele din fiecare subrețea rutează corespunzător către gateway-ul corespunzător pentru a accesa subrețeaua la distanță.

Concepte înrudite

Rutarea TCP/IP și echilibrarea încărcării

Completarea foilor de lucru pentru planificare

Următoarele liste de verificări pentru planificare arată tipul de informații de care aveți nevoie înainte de a începe configurarea VPN. Toate răspunsurile din lista de verificare a cerinței 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.

Tabela 3. Cerințe sistem

| Listă de verificare pentru cerințele preliminare | Răspunsuri |
|--|------------|
| Sistemul dumneavoastră de operare este OS/400 V5R2 (5722-SS1) sau ulterior? | Da |
| Este instalat Digital Certificate Manager (5722-SS1 opțiunea 34)? | Da |
| Este instalat iSeries Access pentru Windows (5722-XE1)? | Da |
| Este instalat Navigator iSeries? | Da |
| Este instalată subcomponenta Rețea din Navigator iSeries? | Da |
| Este instalat TCP/IP Connectivity Utilities (5722-TC1)? | Da |
| Ați setat la 1 valoarea de sistem pentru reținerea datelor de securitate ale serverului (QRETSVRSEC *SEC)? | Da |
| Este configurat TCP/IP pe sistem (inclusiv interfețele IP, rutele, numele de gazdă locală și numele de domeniu local)? | Da |
| Este stabilită comunicația TCP/IP normală între punctele finale cerute? | Da |
| Ați aplicat cele mai recente corecții temporare de program (PTF-uri)? | Da |

Tabela 3. Cerințe sistem (continuare)

| Listă de verificare pentru cerințele 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 și ESP? | Da |
| Sunt configurate firewall-urile sau ruterul pentru a permite protocoalele IKE (UDP port 500), AH și ESP? | Da |
| Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP? | Da |

Tabela 4. Configurație VPN

| Aveți nevoie de aceste informații pentru a configura VPN-ul | Răspunsuri |
|--|--|
| Ce tip de conexiune creați ? | gateway-la-gateway |
| Cum veți denumi grupul de chei dinamice? | HRgw2FINgw |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? | echilibrate |
| Folosiți certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată? | Nu este topsecretstuff |
| Care este identificatorul serverului de chei local? | Adresa IP: 204.146.18.227 |
| Care este identificatorul punctului final de date local ? | Subrețea: 10.6.0.0 Mască: 255.255.0.0 |
| Care este identificatorul serverului de chei la distanță ? | Adresa IP: 208.222.150.250 |
| Care este identificatorul punctului final de date la distanță ? | Subrețea: 10.196.8.0 Mască: 255.255.255.0 |
| Ce porturi și protocoale doriți să permiteți prin conexiune ? | Oricare |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja datele? | echilibrate |
| Pe care dintre interfețe se aplică această conexiune ? | TRLINE |

Configurarea VPN-ului pe iSeries-A

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

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Rețea privată virtuală** și selectați **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
3. Revedeți pagina **Bine ați venit** pentru informații despre ce obiecte creează vrăjitorul.
4. Faceți clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceți MyCo2TheirCo.
6. Opțional: Specificați o descriere pentru acest grup de conexiuni.
7. Faceți clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectați **Conectarea gazdei dumneavoastră la altă gazdă**.
9. Faceți clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectați **Crearea unei noi politici** și apoi selectați **Cea mai înaltă securitate, cea mai joasă performanță**.
11. Apăsați pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectați **Da** pentru a indica dacă veți folosi certificate pentru autentificarea conexiunii. Apoi, selectați certificatele care reprezintă iSeries A.

Notă: Dacă vreți să folosiți un certificat pentru autentificarea punctului final al conexiunii locale, trebuie să creați întâi certificatul în DCM.

13. Apăsați **Următor** pentru a merge în pagina **Identificator de punct final al conexiunii locale**.

14. Selectați **Adresa IP Versiunea 4** ca tip de identificator. Adresa IP asociată trebuie să fie 10.6.1.1. Din nou, aceste informații sunt definite în certificatul pe care îl creați în DCM.
15. Apăsați **Următor** pentru a merge la pagina **Server de chei la distanță**.
16. Selectați **Adresa IP Versiunea 4** din câmpul **Tip de identificator**.
17. Introduceți 10.196.8.6 în câmpul **Identificator**.
18. Apăsați **Următor** pentru a merge în pagina **Servicii de date**.
19. Acceptați valorile implicite și apoi apăsați **Următor** pentru a merge în pagina **Politică de date**.
20. Selectați **Crearea unei noi politici** și apoi selectați **Cea mai înaltă securitate, cea mai joasă performanță**. Selectați **Folosirea algoritmului de criptare RC4**.
21. Apăsați **Următor** pentru a merge la pagina **Interfețe aplicabile**.
22. Selectați **TRLINE**.
23. Apăsați **Următor** pentru a merge la pagina **Sumar**. Revedeți obiectele pe care le va crea pentru a asigura corectitudinea lor.
24. Apăsați pe **Sfârșit** pentru a termina configurarea.
25. Când apare caseta de dialog **Activare filtre politică**, selectați **Nu, regulile pachet vor fi activate la un moment ulterior** apoi faceți clic pe **Ok**.

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

1. Faceți clic pe **După grup** în panoul din stânga al interfeței VPN și grupul nou de chei dinamice, MyCo2TheirCo, va fi afișat în panoul din dreapta. Faceți clic dreapta pe el și selectați **Proprietăți**.
2. Mergeți la pagina **Politică** și selectați opțiunea **Sistemul local inițiază conexiunea**.
3. Apăsați **OK** pentru a salva modificările.

Configurarea VPN-ului pe iSeries-C

Parcurgeți aceiași pași ca la configurarea VPN-ului pe iSeries-A, înlocuind adresele IP după cum e necesar. Folosiți ca ghid foile de lucru pentru planificare. După ce terminați de configurat gateway-ul VPN al departamentului Finanțe, 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 porniți serverele VPN, dacă nu sunt deja pornite.

Activarea de reguli pachete

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

1. În Navigator iSeries, expandați **iSeries-A → Rețea → Politici IP**.
2. Faceți clic dreapta pe **Reguli pachete** și selectați **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectați dacă vreți să activați doar regulile generate VPN, doar un fișier selectat sau ambele variante. Puteți alege ultima variantă, de exemplu, dacă aveți diverse reguli PERMIT și DENY pe care doriți să le impuneți pe interfață în plus față de regulile generate VPN.
4. Selectați interfața pe care vreți să activați regulile. În acest caz, selectați **Toate interfețele**.
5. Faceți clic pe **OK** în caseta de dialog pentru a confirma ca vreți să verificați și să activați regulile pe interfața sau interfețele specificate. După ce ați apăsat OK, sistemul verifică regulile de erori sintactice și semantice și raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fișier anume și un număr de linie, puteți apăsa clic dreapta pe eroare și selecta **Mergi la linie** pentru a evidenția eroarea în fișier.
6. Repetați acești pași pentru a activa regulile de pachete pe iSeries C.

Pornirea conexiunii

Parcurgeți pașii următori pentru a porni conexiunea MyCo2TheirCo de la iSeries-A:

1. În Navigator iSeries, expandați **iSeries-A** → **Rețea** → **Politici IP**.
2. Dacă serverul VPN nu este pornit, faceți clic dreapta pe **Rețea privată virtuală** și selectați **Pornire**. Aceasta pornește serverul VPN.
3. Expandați **VPN** → **Conexiuni securizate**.
4. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
5. Faceți clic dreapta pe **MyCo2TheirCo** și selectați **Pornire**.
6. Din meniul **Vizualizare**, selectați **Reîmprospătare**. Dacă conexiunea pornește cu succes, starea se va modifica din *Inactivă* în *Activată*. Pot trece câteva minute până pornește conexiunea, așa că trebuie să reîmprospătați periodic până când starea se schimbă la *Activată*.

Testarea conexiunii

După ce ați terminat de configurat ambele servere și ați pornit cu succes serverele VPN, testați conectivitatea pentru a vă asigura că subrețelele la distanță pot comunica una cu cealaltă. Pentru aceasta, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **iSeries-A** → **Rețea**.
2. Faceți clic dreapta pe **Configurarea TCP/IP** și selectați **Utilitare** și apoi selectați **Ping**.
3. Din caseta de dialog **Ping de la**, introduceți iSeries-C în câmpul **Ping**.
4. Faceți clic pe **Ping acum** pentru verificarea conectivității de la iSeries-A la iSeries-C.
5. Faceți clic pe **OK** când ați terminat.

Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec

În acest scenariu, aflați cum să setați o conexiune între o gazdă a filialei și sediul central care folosește L2TP protejat de IPSec. Biroul filialei are o adresă IP alocată dinamic, în timp ce biroul companiei are o adresă IP statică, rutabilă global.

Situație

Să presupunem că compania dumneavoastră are un mic birou de filială în alt stat. În orice zi de lucru filiala poate necesita acces la informațiile confidențiale de pe un sistem iSeries din intranetul companiei. Compania dumneavoastră folosește în prezent o linie închiriată scumpă pentru a furniza accesul biroului filială la rețeaua companiei. Deși compania dumneavoastră dorește să asigure în continuare un acces sigur la intranet, în ultimă în cele din urmă doriți să reduceți 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 rețeaua companiei, astfel ca biroul filialei să apară ca o parte a subrețelei companiei. VPN protejează traficul de date prin tunelul L2TP.

Cu un tunel voluntar L2TP, biroul filialei de la distanță stabilește un tunel direct la serverul de rețea L2TP (LNS) al rețelei companiei. Funcționalitatea concentratorului de acces L2TP (LAC) se află la client. Tunelul este transparent pentru furnizorul de servicii Internet (ISP) al clientului de la distanță, astfel că ISP-ul nu trebuie să suporte L2TP. Dacă vreți să citiți mai multe despre conceptele L2TP, vedeți L2TP (Layer 2 Tunnel Protocol).

Important: Acest scenariu arată gateway-urile de securitate atașate direct la Internet. Absența unui firewall are intenția de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luați în considerare riscurile de securitate implicate de fiecare dată când vă conectați la Internet.

Obiective

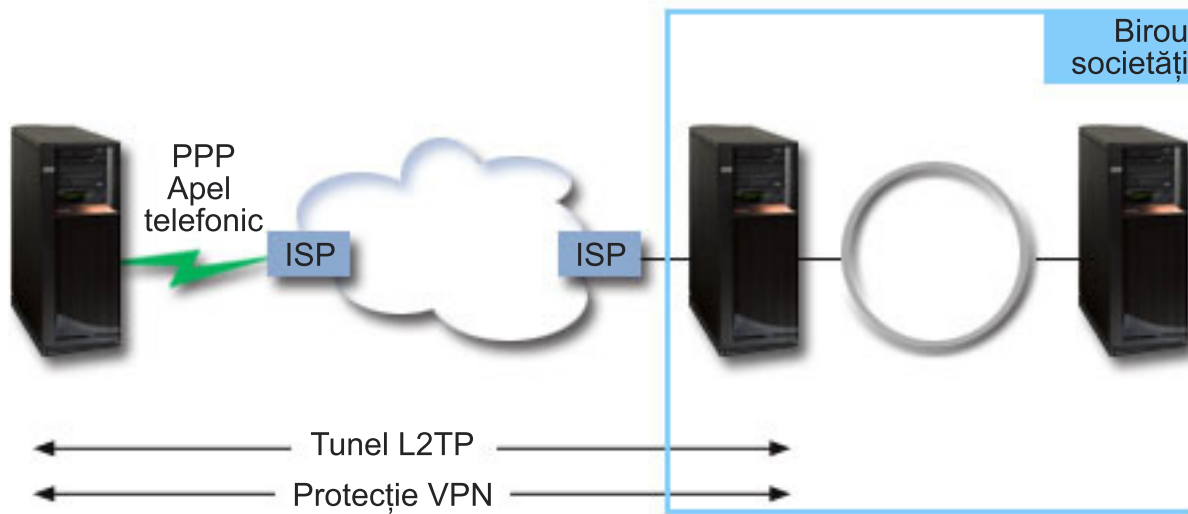
În acest scenariu, un sistem al filialei se conectează la rețeaua companiei printr-un sistem gateway cu un tunel L2TP protejat de VPN.

Obiectivele principale ale acestui scenariu sunt:

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

Detalii

Următoarea ilustrați prezintă caracteristicile rețelei pentru acest scenariu:



iSeries-A

- Trebuie să aibă acces la aplicațiile TCP/IP pe toate sistemele din rețeaua companiei.
- Primește adrese IP alocate dinamic de la ISP-ul său.
- Trebuie să fie configurat să furnizeze suport L2TP.

iSeries-B

- Trebuie să aibă acces la aplicații TCP/IP de pe iSeries-A.
- Subrețeaua este 10.6.0.0 cu masca 255.255.0.0. Această subrețea 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 și aplică IPSec la datagrammele IP care intră și care ies. iSeries-B se conectează la subrețeaua sa cu adresa IP 10.6.11.1.

În termeni L2TP, *iSeries-A* funcționează ca inițiatorul L2TP, în timp ce *iSeries-B* funcționează ca terminator L2TP.

Task-urile de configurare

Presupunând că deja există și funcționează configurarea TCP/IP, trebuie să executați următoarele operații:

Concepte înrudite

“Layer 2 Tunnel Protocol (L2TP)” la pagina 8

Folosiți aceste informații pentru a afla despre crearea unei conexiuni VPN pentru a securiza comunicațiile între rețeaua dumneavoastră și clienții de la distanță.

Informații înrudite

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

Configurarea VPN-ului pe iSeries-A

Urmați acești pași pentru a configura VPN-ul pe iSeries-A:

1. Configurarea politicii Internet Key Exchange

- a. În Navigator iSeries, expandați iSeries-A → **Rețea** → **Politici IP** → **VPN** → **Politici IPsec**.
- b. Faceți clic dreapta pe **Politici Internet Key Exchange** și selectați **Politică nouă Internet Key Exchange**.
- c. În pagina **Server la distanță**, selectați **Adresă IP Versiunea 4** drept tipul de identificator și apoi introduceți 205.13.237.6 în câmpul **Adresa IP**.
- d. În pagina **Asocieri**, selectați **Cheie prepartajată** pentru a indica faptul că această conexiune folosește o cheie prepartajată pentru a autentifica această politică.
- e. Introduceți cheia prepartajată în câmpul **Cheie**. Tratați cheia prepartajată ca pe o parolă.
- f. Selectați **Identificator cheie** pentru tipul identificatorului serverului de chei local și apoi introduceți identificatorul cheii în câmpul **Identificator**. De exemplu, thisisthekeyid. Rețineți că serverul de chei local are o adresă IP atribuită dinamic, care este imposibil de cunoscut înainte. iSeries-B folosește acest identificator pentru a identifica iSeries-A când iSeries-A inițiază o conexiune.
- g. În pagina **Transformări**, apăsați **Adăugare** pentru a adăuga transformări pe care iSeries-A le propune lui iSeries-B pentru protecția cheilor și pentru a specifica dacă politica IKE folosește protecția identității când inițiază negocierile din faza 1.
- h. În pagina **Transformare politică IKE**, selectați **Cheie prepartajată** pentru metoda de autentificare, **SHA** pentru algoritmul hash și **3DES-CBC** pentru algoritmul de criptare. Acceptați valorile implicite pentru grupul Diffie-Hellman și pentru Expirare chei IKE după.
- i. Apăsați **OK** pentru a reveni la pagina **Transformări**.
- j. Selectați **Negociere în mod agresiv IKE (fără protecție de identitate)**.

Notă: Dacă folosiți chei prepartajate și negociere în modul agresiv în configurația dumneavoastră, selectați pentru parole cuvinte necunoscute, pentru care este mică probabilitatea de a fi sparte în atacurile care scanează un dicționar. Se recomandă de asemenea să vă modificați periodic parolele.

- k. Apăsați **OK** pentru a salva configurația.

2. Configurare politică de date

- a. Din interfața VPN, faceți clic dreapta pe **Politici de date** și selectați **Politică nouă de date**.
- b. În pagina **General**, specificați numele politicii de date. De exemplu, l2tpremoteuser.
- c. Mergeți la pagina **Propuneri**. O propunere este o colecție de protocoale pe care le folosesc serverele de chei inițiatoare și respondente pentru a stabili o conexiune dinamică între două capete. Puteți folosi o singură politică de date în mai multe obiecte conexiune. Însă nu toate serverele de chei VPN la distanță trebuie neapărat să aibă aceleași proprietăți pentru politica de date. De aceea, puteți adăuga mai multe propuneri pentru aceeași politică de date. La stabilirea unei conexiuni cu un server la distanță, trebuie să fie cel puțin o propunere corespunzătoare în politica de date a inițiatorului și respondentului.
- d. Apăsați **Adăugare** pentru a adăuga o transformare de politică de date.
- e. Selectați **Transport** pentru modul de încapsulare.
- f. Apăsați **OK** pentru a reveni la pagina **Transformări**.
- g. Specificați o valoare pentru expirarea cheii.
- h. Apăsați **OK** pentru a salva noua politică de date.

3. Configurarea grupului de chei dinamice

- a. Din interfața VPN, expandați **Conexiuni securizate**.
- b. Faceți clic dreapta pe **După grup** și selectați **Grup nou de chei dinamice**.
- c. În pagina **General**, specificați un nume pentru grup. De exemplu, l2tpcorp.
- d. Selectați **Protejare tunel L2TP inițiat local**.
- e. Pentru rolul sistemului, selectați **Ambele sisteme sunt gazde**.

- f. Mergeți la pagina **Politică**. Selectați politica de date pe care ați creat-o la pasul **Configurarea politicii de date**, l2tpremoteuser, din lista **Politică de date**.
 - g. Selectați **Sistemul local inițiază conexiunea** pentru a indica faptul că doar iSeries-A poate iniția conexiuni cu iSeries-B.
 - h. Mergeți la pagina **Conexiuni**. Selectați **Generare următoarea regulă de filtrare politici pentru acest grup**. Apăsați **Editare** pentru a defini parametrii filtrului de politici.
 - i. În pagina **Filtru de politică - Adrese locale**, selectați **Identificator cheie** drept tipul identificatorului.
 - j. Pentru identificator, selectați identificatorul de cheie, thisisthekeyid, pe care l-ați definit în politica IKE.
 - k. Mergeți la pagina **Filtru politică - Adrese la distanță**. Selectați **Adresă IP Versiunea 4** din lista **Tip identificator**.
 - l. Introduceți 205.13.237.6 în câmpul **Identificator**.
 - m. Mergeți la pagina **Filtru politică - Servicii**. Introduceți 1701 în câmpurile **Port local** și **Port la distanță**. Portul 1701 este binecunoscutul port pentru L2TP.
 - n. Selectați **UDP** din lista **Protocol**.
 - o. Apăsați **OK** pentru a reveni la pagina **Conexiuni**.
 - p. Mergeți la pagina **Interfețe**. Selectați orice profil linie sau PPP pentru care se va aplica acest grup. Încă nu ați creat profilul PPP pentru acest grup. După ce faceți acest lucru, va trebui să editați proprietățile acestui grup astfel încât grupul să se aplice pentru profilul PPP pe care îl creați în pasul următor.
 - q. Apăsați **OK** pentru a crea grupul de chei dinamice, l2tpcorp.
4. **Configurarea conexiunii cu chei dinamice**
- a. Din interfața VPN, expandați **După grup**. Aceasta afișează o listă cu toate grupurile de chei dinamice pe care le-ați configurat pe iSeries-A.
 - b. Faceți clic dreapta pe **l2tpcorp** și selectați **Conexiune nouă cu chei dinamice**.
 - c. În pagina **General**, specificați o descriere opțională a conexiunii.
 - d. Pentru serverul de chei la distanță, selectați **Adresă IP v4** pentru tipul identificatorului.
 - e. Selectați 205.13.237.6 din lista **Adresa IP**.
 - f. Deselectați **Pornire la-cerere**.
 - g. Mergeți la pagina **Adrese locale**. Selectați **Identificator cheie** pentru tipul identificatorului și apoi selectați thisisthekeyid din lista **Identificator**.
 - h. Mergeți la pagina **Adrese la distanță**. Selectați **Adresă IP Versiunea 4** pentru tipul identificatorului.
 - i. Introduceți 205.13.237.6 în câmpul **Identificator**.
 - j. Mergeți la pagina **Servicii**. Introduceți 1701 în câmpurile **Port local** și **Port la distanță**. Portul 1701 este binecunoscutul port pentru L2TP.
 - k. Selectați **UDP** din lista **Protocol**.
 - l. Apăsați **OK** pentru a crea conexiunea cu cheie dinamică.

Configurarea unui profil de conexiune PPP și linie virtuală pentru iSeries-A

Această secțiune descrie pașii pe care trebuie să-i urmați pentru a crea profilul PPP pentru iSeries-A. Profilul PPP nu are o linie fizică asociată cu el; el folosește o linie virtuală. Aceasta deoarece traficul PPP trece prin tunelul L2TP, în timp ce VPN protejează tunelul L2TP.

Urmați acești pași pentru a crea un profil de conexiune PPP pentru iSeries-A:

1. În Navigator iSeries, expandați iSeries-A → **Rețea** → **Servicii de acces la distanță**.
2. Faceți clic dreapta pe **Profiluri de conexiune inițiator** și selectați **Profil nou**.
3. În pagina **Setare**, selectați **PPP** pentru tipul protocolului.
4. Pentru Selecții mod, selectați **L2TP (linie virtuală)**.
5. Selectați **Inițiator la-cerere (tunel voluntar)** din lista derulantă **Mod operare**.
6. Apăsați **OK** pentru a merge la pagina cu proprietăți profiluri PPP.

7. În pagina **General**, introduceți un nume care identifică tipul și destinația conexiunii. În acest caz, introduceți toCORP. Numele trebuie pe care îl specificați trebuie să fie de 10 caractere sau mai puțin.
8. Opțional: Specificați o descriere pentru profil.
9. Mergeți la pagina **Conexiune**.
10. În câmpul **Nume linie virtuală**, selectați **tocorp** din lista derulantă. Țineți minte că această linie nu are interfețe fizice asociate. Linia virtuală descrie diferite caracteristici ale acestui profil PPP; de exemplu, dimensiunea maximă a cadrului, informații despre autentificare, nume gazdă local etc. Apare caseta de dialog **Proprietăți linie L2TP**.
11. În pagina **General**, introduceți o descriere pentru linia virtuală.
12. Mergeți la pagina **Autentificare**.
13. În câmpul **Nume gazdă locală**, introduceți numele de gazdă al serverului local de chei, iSeriesA.
14. Apăsați **OK** pentru a salva descrierea liniei virtuale noi și reveniți la pagina **Conexiune**.
15. Introduceți adresa punctului final al tunelului de la distanță, 205.13.237.6, în câmpul **Adresă punct final tunel la distanță**.
16. Selectați **Este necesară protecția IPSec** și selectați grupul de chei dinamice pe care l-ați creat în pasul anterior "Configurarea VPN-ului pe iSeries-A" la pagina 24, l2tptocorp din lista derulantă **Nume grup conexiune**.
17. Mergeți la pagina **Setări TCP/IP**.
18. În secțiunea **Adresă IP locală**, selectați **Atribuită de sistem de la distanță**.
19. În secțiunea **Adresă IP la distanță**, selectați **Folosire adresă IP fixă**. Introduceți 10.6.11.1, care este adresa IP a sistemului de la distanță din subrețeaua sa.
20. În secțiunea de rutare, selectați **Definire rute statice suplimentare** și apăsați **Rute**. Dacă nu este furnizată nici o informație de rutare în profilul PPP, atunci iSeries-A poate să ajungă doar la punctul final al tunelului de la distanță, dar la nici un alt sistem de pe subrețeaua 10.6.0.0.
21. Apăsați **Adăugare** pentru a adăuga o intrare de rută statică.
22. Introduceți subrețeaua, 10.6.0.0 și masca subrețelei, 255.255.0.0 pentru a ruta tot traficul 10.6.*.* prin tunelul L2TP.
23. Apăsați **OK** pentru a adăuga ruta statică.
24. Faceți clic pe **OK** pentru a închide caseta de dialog Rutare.
25. Mergeți la pagina **Autentificare** pentru a seta numele utilizatorului și parola pentru acest profil PPP.
26. În secțiunea Identificare sistem local, selectați **Permitere sistemului de la distanță să verifice identitatea acestui sistem**.
27. Sub **Protocol de autentificare de folosit** selectați **Este necesară parolă criptată (CHAP-MD5)**. În secțiunea Identificare sistem local, selectați **Permitere sistemului de la distanță să verifice identitatea acestui sistem**.
28. Introduceți numele utilizatorului, iSeriesA, și o parolă.
29. Apăsați **OK** pentru a salva profilul PPP.

Aplicarea grupului de chei dinamice l2tptocorp la profilul PPP toCorp

După ce ați configurat profilul de conexiune PPP, trebuie să mergeți înapoi la grupul de chei dinamice, l2tptocorp, pe care l-ați creat și să îl asociați cu profilul PPP. Pentru aceasta, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate** → **După grup**.
2. Faceți clic dreapta pe grupul de chei dinamice, l2tptocorp, și selectați **Proprietăți**.
3. Mergeți la pagina **Interfețe** și selectați **Aplicare acest grup** pentru profilul PPP pe care l-ați creat în pasul "Configurarea unui profil de conexiune PPP și linie virtuală pentru iSeries-A" la pagina 25, toCorp.
4. Apăsați **OK** pentru a aplica l2tptocorp la profilul PPP, toCorp.

Configurarea VPN-ului pe iSeries-B

Urmați aceiași pași pe care i-ați utilizat pentru "Configurarea VPN-ului pe iSeries-A" la pagina 24, înlocuind adresele IP și identicatorii după cum este cazul. Luați în calcul și aceste puncte înainte să începeți:

- Identificați serverul de chei la distanță prin identificatorul cheie pe care l-ați specificat pentru serverul de chei local pe iSeries-A. De exemplu, `thisisthekeyid`.
- Folosiți *exact* aceeași cheie prepartajată.
- Asigurați-vă că transformările dumneavoastră corespund cu cele pe care le-ați configurat pe iSeries-A sau conexiunile vor eșua.
- Nu specificați **Protejare tunel L2TP inițiat local** pe pagina **General** a grupului de chei dinamice.
- Sistemul la distanță inițiază conexiunea.
- Specificați pornirea la cerere a conexiunii.

Configurarea unui profil de conexiune PPP și linie virtuală pentru iSeries-B

Urmați acești pași pentru a crea un profil de conexiune PPP pentru iSeries-B:

1. În Navigator iSeries, expandați iSeries-B → **Rețea** → **Servicii de acces la distanță**.
2. Faceți clic dreapta pe **Profiluri de conexiune respondent** și selectați **Profil nou**.
3. În pagina **Setare**, selectați **PPP** pentru tipul protocolului.
4. Pentru Selecții mod, selectați **L2TP (linie virtuală)**.
5. Selectați **Terminator (server de rețea)** din lista **Modul de operare**.
6. Apăsați **OK** pentru pagina **Proprietăți profiluri PPP**.
7. În pagina **General**, introduceți un nume care identifică tipul și destinația conexiunii. În acest caz, introduceți **tobranch**. Numele trebuie pe care îl specificați trebuie să fie de 10 caractere sau mai puțin.
8. Opțional: Specificați o descriere pentru profil
9. Mergeți la pagina **Conexiune**.
10. Selectați adresa IP a punctului final local al tunelului, 205.13.237.6.
11. În câmpul **Nume linie virtuală**, selectați **tobranch** din lista derulantă. Țineți minte că această linie nu are interfețe fizice asociate. Linia virtuală descrie diferite caracteristici ale acestui profil PPP; de exemplu, dimensiunea maximă a cadrului, informații despre autentificare, nume gazdă local etc. Apare caseta de dialog **Proprietăți linie L2TP**.
12. În pagina **General**, introduceți o descriere pentru linia virtuală.
13. Mergeți la pagina **Autentificare**.
14. În câmpul **Nume gazdă locală**, introduceți numele de gazdă al serverului local de chei, iSeriesB.
15. Apăsați **OK** pentru a salva descrierea liniei virtuale noi și reveniți la pagina **Conexiune**.
16. Mergeți la pagina **Setări TCP/IP**.
17. În secțiunea **Adresă IP locală**, selectați adresa IP fixă a sistemului local, 10.6.11.1.
18. În secțiunea **Adresă IP la distanță**, selectați **Pool de adrese** ca metodă de atribuire a adresei. Introduceți o adresă de pornire și apoi specificați numărul de adrese care pot să fie atribuite sistemului la distanță.
19. Selectați **Permitere sistemului de la distanță să acceseze alte rețele (înaintare IP)**.
20. Mergeți la pagina **Autentificare** pentru a seta numele utilizatorului și parola pentru acest profil PPP.
21. În secțiunea **Identificare sistem local**, selectați **Permitere sistemului de la distanță să verifice identitatea acestui sistem**. Aceasta deschide caseta de dialog **Identificare sistem local**.
22. Sub **Protocol de autentificare de folosit** selectați **Este necesară parolă criptată (CHAP-MD5)**.
23. Introduceți numele utilizatorului, iSeriesB, și o parolă.
24. Apăsați **OK** pentru a salva profilul PPP.

Activarea de reguli pachete

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

1. În Navigator iSeries, expandați iSeries-A → **Rețea** → **Politici IP**.

2. Faceți clic dreapta pe **Reguli pachete** și selectați **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectați dacă vreți să activați doar regulile generate VPN, doar un fișier selectat sau ambele variante. Puteți alege ultima variantă, de exemplu, dacă aveți diverse reguli PERMIT și DENY pe care doriți să le impuneți pe interfață în plus față de regulile generate VPN.
4. Selectați interfața pe care vreți să activați regulile. În acest caz, selectați **Toate interfețele**.
5. Faceți clic pe **OK** în caseta de dialog pentru a confirma ca vreți să verificați și să activați regulile pe interfața sau interfețele specificate. După ce ați apăsat OK, sistemul verifică regulile de erori sintactice și semantice și raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fișier anume și un număr de linie, puteți apăsa clic dreapta pe eroare și selecta **Mergi la linie** pentru a evidenția eroarea în fișier.
6. Repetați acești pași pentru a activa regulile de pachete pe iSeries-B.

| Scenariu: VPN prietenos pentru firewall

| În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago și o gazdă din Minneapolis, atunci când amândouă serverele sunt în spatele unui firewall.

| Situație

| Presupunem că sunteți o mare companie de asigurări pentru locuințe cu sediul în Minneapolis și ați deschis de curând o filială la Chicago. Filiala din Chicago are nevoie să acceseze baza de date a clienților care se află la sediul central din Minneapolis. Vreți să fiți siguri că informațiile transferate sunt securizate, deoarece baza de date conține date confidențiale despre clienții dumneavoastră, cum ar fi: numele, adresele și numerele de telefon. Decideți să conectați cele două sedii prin internet folosind VPN (Virtual Private Network). Amândouă părțile sunt în spatele unui firewall și folosesc NAT (translatarea adreselor de rețea), pentru a ascunde adresele IP private neînregistrate în spatele unui set de adrese IP înregistrate. Dar, conexiunile VPN au câteva incompatibilități bine cunoscute cu NAT. O conexiune VPN ignoră pachetele trimise printr-un dispozitiv NAT, deoarece NAT modifică adresa IP a pachetului, prin aceasta invalidând pachetul. Totuși, puteți folosi o conexiune VPN cu NAT dacă implementați încapsularea UDP.

| În acest scenariu adresa IP din rețeaua Chicago este pusă într-un nou antet IP și este translatată când trece prin Firewall-C (vedeți următoarea imagine). Apoi, pachetul ajunge la Firewall-D, el va traduce adresa IP destinație la adresa IP Sistem-E, prin urmare pachetul va fi înaintat la Sistem-E. La final, când pachetul ajunge la Sistem-E, i se scoate antetul UDP, păstrându-se pachetul IPSec original, care va fi supus acum la toate validările și care permite o conexiune VPN securizată.

| Obiective

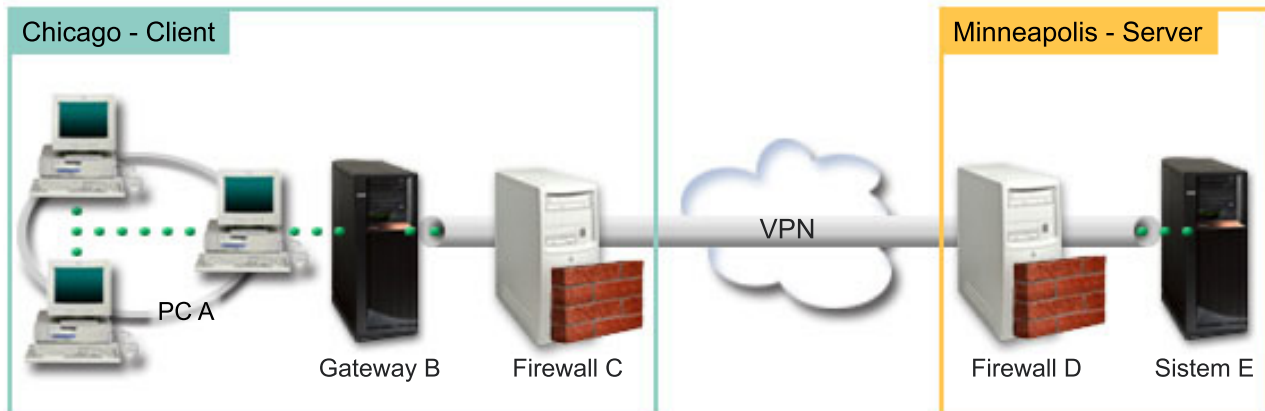
| În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago (client) și o gazdă din Minneapolis (server), atunci când amândouă rețelele sunt în spatele unui firewall.

| Obiectivele acestui scenariu sunt următoarele:

- Gateway-ul filialei din Chicago inițiază întotdeauna conexiunea la gazda din Minneapolis.
- VPN trebuie să protejeze tot traficul de date între gateway-ul din Chicago și gazda din Minneapolis.
- Să se permită tuturor utilizatorilor gateway-ului din Chicago, printr-o conexiune VPN, să acceseze o bază de date iSeries aflată în rețeaua din Minneapolis.

Detalii

Următoarea ilustrați prezintă caracteristicile rețelei pentru acest scenariu:



Rețeaua Chicago - Client

- iSeries Gateway-B rulează pe i5/OS Versiunea 5 Ediția 4 (V5R4)
- Gateway-B se conectează la internet cu adresa IP 214.72.189.35 și este punctul final al conexiunii pentru tunelul VPN. Gateway-B realizează negocierile IKE și aplică încapsularea UDP datagramelor IP de ieșire.
- Gateway-B și PC-A sunt în subrețeaua 10.8.11.0 cu masca 255.255.255.0
- PC-A este sursă și destinație pentru datele care circulă prin conexiunea VPN, de aceea este punctul final de date al tunelului VPN.
- Doar Gateway-B poate iniția conexiunea cu Sistem-E.
- Firewall-C are o regulă Masq NAT cu adresa IP publică 129.42.105.17, care ascunde adresa IP pentru Gateway-B

Rețeaua Minneapolis - Server

- iSeries Sistem-E rulează pe i5/OS Versiunea 5 Ediția 4 (V5R4)
- Sistem-E are adresa IP 56.172.1.1.
- Sistem-E este respondentul pentru acest scenariu.
- Firewall-D are adresa IP 146.210.18.51.
- Firewall-D are o regulă Static NAT care mapează adresa IP publică (146.210.18.15) la adresa IP privată pentru Sistem-E (56.172.1.1). Prin urmare, din perspectiva clientului adresa IP pentru Sistem-E este adresa IP publică (146.210.18.51) pentru Firewall-D.

Task-urile de configurare

Concepte înrudite

“Gestionarea cheilor” la pagina 6

Un VPN dinamic furnizează securitate suplimentară pentru comunicațiile 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.

“IPSec compatibil NAT cu UDP” la pagina 10

Încapsularea UDP permite traficului IPSec să treacă printr-un dispozitiv NAT convențional. Treceți în revistă acest subiect pentru mai multe informații despre ce este și de ce ar trebui să îl folosiți pentru conexiunile dumneavoastră VPN.

Completarea foilor de lucru pentru planificare

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

Notă: Există foi de lucru separate pentru Gateway-B și Sistem-E.

Tabela 5. Cerințe sistem

| Listă de verificare pentru cerințele preliminare | Răspunsuri |
|--|------------|
| Sistemul dumneavoastră de operare este i5/OS V5R4 (5722-SS1)? | Da |
| Este instalat Digital Certificate Manager (5722-SS1 opțiunea 34)? | Da |
| Este instalat iSeries Access pentru Windows (5722-XE1)? | Da |
| Este instalat Navigator iSeries? | Da |
| Este instalată subcomponenta Rețea din Navigator iSeries? | Da |
| Este instalat TCP/IP Connectivity Utilities (5722-TC1)? | Da |
| Ați setat la 1 valoarea de sistem pentru reținerea datelor de securitate ale serverului (QRETSVRSEC *SEC)? | Da |
| Este configurat TCP/IP pe sistem (inclusiv interfețele IP, rutele, numele de gazdă locală și numele de domeniu local)? | Da |
| Este stabilită comunicația TCP/IP normală între punctele finale cerute? | Da |
| Ați aplicat cele mai recente corecții 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 și ESP? | Da |
| Sunt configurate firewall-urile sau ruterile pentru a permite traficul prin porturile 4500 pentru negocierea cheilor? Tipic, partenerii VPN realizează negocieri IKE prin UDP port 500, când IKE detectează că pachetele NAT sunt trimise peste portul 4500. | Da |
| Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP? | Da |

Tabela 6. Configurație gateway-B

| Aveți nevoie de aceste informații pentru a configura VPN pentru Gateway-B | Răspunsuri |
|--|---|
| Ce tip de conexiune creați ? | gateway-la-altă gazdă |
| Cum veți denumi grupul de chei dinamice? | CHIGw2MINhost |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? | echilibrate |
| Folosiți certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată? | Nu : topsecretstuff |
| Care este identificatorul serverului de chei local? | Adresa IP: 214.72.189.35 |
| Care este identificatorul punctului final de date local ? | Subrețea: 10.8.11.0 Mască: 255.255.255.0 |
| Care este identificatorul serverului de chei la distanță ? | Adresa IP: 146.210.18.51 |
| Care este identificatorul punctului final de date la distanță ? | Adresa IP: 146.210.18.51 |
| Ce porturi și protocoale doriți să permiteți prin conexiune ? | Oricare |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja datele? | echilibrate |
| Pe care dintre interfețe se aplică această conexiune ? | TRLINE |

Tabela 7. Configurație Sistem-E

| Aveți nevoie de aceste informații pentru a configura VPN pentru Sistem-E | Răspunsuri |
|--|---|
| Ce tip de conexiune creați ? | gază-la-alt gateway |
| Cum veți denumi grupul de chei dinamice? | CHlgw2MINhost |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? | cele mai înalte |
| Folosiți certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată? | Nu : topsecretstuff |
| Care este identificatorul serverului de chei local? | Adresa IP: 56.172.1.1 |
| Care este identificatorul serverului de chei la distanță? Notă: Dacă adresa IP pentru Firewall-C este necunoscută, puteți folosi *ANYIP ca identificator pentru serverul de chei de la distanță. | Adresa IP: 129.42.105.17 |
| Care este identificatorul punctului final de date la distanță ? | Subrețea: 10.8.11.0 Mască: 255.255.255.0 |
| Ce porturi și protocoale doriți să permiteți prin conexiune ? | Oricare |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja datele? | cele mai înalte |
| Pe care dintre interfețe se aplică această conexiune ? | TRLINE |

Configurarea VPN pe Gateway-B

Folosiți informațiile din foile dumneavoastră de lucru pentru a configura VPN-ul pe Gateway-B, după cum urmează:

- În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
- Faceți clic dreapta pe **Rețea privată virtuală** și selectați **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
- Revedeți pagina **Bine ați venit** pentru informații despre ce obiecte creează vrăjitorul.
- Faceți clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
- În câmpul **Nume**, introduceți CHlgw2MINhost.
- Opțional: Specificați o descriere pentru acest grup de conexiuni.
- Faceți clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
- Selectați **Conectarea gateway-ului dumneavoastră la altă gazdă**.
- Faceți clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
- Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.

Notă: Dacă primiți un mesaj de eroare care spune "Cererea de certificat nu a putut fi procesată" puteți să-l ignorați, deoarece nu folosiți certificate pentru schimbul de chei.

- Opțional: Dacă aveți certificate instalate veți vedea pagina **Certificat pentru punctul final al conexiunii locale**. Selectați Nu pentru a indica că nu veți folosi certificate pentru a autentifica conexiunea.
- Apăsați **Următor** pentru a merge la pagina **Server de chei local**.
- Selectați **IP versiunea 4** din câmpul **Tip identificator**.
- Selectați 214.72.189.35 din câmpul **Adresă IP**.
- Apăsați **Următor** pentru a merge la pagina **Server de chei la distanță**.
- Selectați **Adresă IP versiunea 4** în câmpul **Tip identificator**.
- Introduceți 146.210.18.51 în câmpul **Identificator**.

Notă: Dacă gateway-ul B inițiază o conexiune la un Static NAT trebuie să specificați modul principal de schimbare de chei pentru a introduce o singură adresă IP pentru cheia de la distanță. Modul principal de schimb de chei este selectat implicit când creați o conexiune cu vrăjitorul de conexiuni VPN. Dacă este folosit modul agresiv în această situație, trebuie introdus pentru cheia de la distanță un tip de identificator la distanță diferit de IPV4.

- Introduceți topsecretstuff în câmpul **Cheie prepartajată**.

- | 19. Apăsați **Următor** pentru a merge la pagina **Punct final local de date**.
- | 20. Selectați **Subrețea IP versiunea 4** din câmpul **Tip identificator**.
- | 21. Introduceți 10.8.0.0 în câmpul **Identificator**.
- | 22. Introduceți 255.255.255.0 în câmpul **Mască subrețea**.
- | 23. Apăsați **Următor** pentru a merge în pagina **Servicii de date**.
- | 24. Acceptați valorile implicite și apoi apăsați **Următor** pentru a merge la pagina **Politică de date**.
- | 25. Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.
- | 26. Apăsați **Următor** pentru a merge la pagina **Interfețe aplicabile**.
- | 27. Selectați **TRLINE** din tabelul **Linie**.
- | 28. Apăsați **Următor** pentru a merge la pagina **Sumar**.
- | 29. Revedeți obiectele pe care le va crea pentru a asigura corectitudinea lor.
- | 30. Apăsați pe **Sfârșit** pentru a termina configurarea.
- | 31. Când apare caseta de dialog **Activare filtre politică**, selectați **Da**, activare filtre de politică generate, apoi selectați **Permitere totală a celui alt trafic**.
- | 32. Apăsați **OK** pentru a încheia configurarea.

| Configurarea VPN pe Sistem-E

| Folosiți informațiile din foile dumneavoastră de lucru pentru a configura VPN pe Sistem-E, după cum urmează:

- | 1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
- | 2. Faceți clic dreapta pe **Rețea privată virtuală** și selectați **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
- | 3. Revedeți pagina **Bine ați venit** pentru informații despre ce obiecte creează vrăjitorul.
- | 4. Faceți clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
- | 5. În câmpul **Nume**, introduceți CHlgw2MINhost.
- | 6. Opțional: Specificați o descriere pentru acest grup de conexiuni.
- | 7. Faceți clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
- | 8. Selectați **Conectarea gazdei dumneavoastră la alt gateway**.
- | 9. Faceți clic pe **Următor** pentru a merge la pagina **Politică Internet Key Exchange**.
- | 10. Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.

| **Notă:** Dacă primiți un mesaj de eroare care spune "Cererea de certificat nu a putut fi procesată" puteți să-l ignorați, deoarece nu folosiți certificate pentru schimbul de chei.

- | 11. Opțional: Dacă aveți certificate instalate veți vedea pagina **Certificat pentru punctul final al conexiunii locale**. Selectați **Nu** pentru a indica că nu veți folosi certificate pentru a autentifica conexiunea.
- | 12. Apăsați **Următor** pentru a merge la pagina **Server de chei local**.
- | 13. Selectați **Adresă IP versiunea 4** în câmpul **Tip identificator**.
- | 14. Selectați 56.172.1.1 din câmpul **Adresă IP**.
- | 15. Apăsați **Următor** pentru a merge la pagina **Server de chei la distanță**.
- | 16. Selectați **Adresă IP versiunea 4** în câmpul **Tip identificator**.
- | 17. Introduceți 129.42.105.17 în câmpul **Identificator**.

| **Notă:** Dacă adresa IP pentru Firewall-C este necunoscută, puteți folosi *ANYIP ca identificator pentru serverul de chei de la distanță.

- | 18. Introduceți topsecretstuff în câmpul **Cheie prepartajată**.
- | 19. Apăsați **Următor** pentru a merge la pagina **Punct final de date distanță**.
- | 20. Selectați **Subrețea IP versiunea 4** din câmpul **Tip identificator**.
- | 21. Introduceți 10.8.11.0 în câmpul **Identificator**.

- | 22. Introduceți 255.255.255.0 în câmpul **Mască subrețea**.
- | 23. Apăsați **Următor** pentru a merge în pagina **Servicii de date**.
- | 24. Acceptați valorile implicite și apoi apăsați **Următor** pentru a merge la pagina Politică de date.
- | 25. Selectați **Creare politică nouă** și apoi selectați **Echilibrare securitate și performanță**.
- | 26. Apăsați **Următor** pentru a merge la pagina **Interfețe aplicabile**.
- | 27. Selectați **TRLINE** din tabelul Linie.
- | 28. Apăsați **Următor** pentru a merge la pagina **Sumar**.
- | 29. Revedeți obiectele pe care le va crea pentru a asigura corectitudinea lor.
- | 30. Apăsați pe **Sfârșit** pentru a termina configurarea.
- | 31. Când apare caseta de dialog **Activare filtre politică**, selectați **Da**, activare filtre de politică generate, apoi selectați **Permitere totală a celuilalt trafic**.
- | 32. Apăsați **OK** pentru a încheia configurarea.

| Pornirea conexiunii

| Urmați acești pași pentru a confirma dacă este activă conexiunea CHIGw2MINhost pe Sistem-E:

- | 1. În Navigator iSeries, expandați **Sistem-E** → **Rețea** → **Conexiuni securizate** → **Toate conexiunile**.
- | 2. Vizualizați **CHIGw2MINhost** și verificați că **Stare** este *Idle* sau *On-Demand*.

| Parcurgeți pașii următori pentru a porni conexiunea CHIGw2MINhost de la Gateway-B:

- | 1. În Navigator iSeries, expandați **Gateway-B** → **Rețea** → **Politici IP**.
- | 2. Dacă serverul VPN nu este pornit, faceți clic dreapta pe **Rețea privată virtuală** și selectați **Pornire**. Aceasta pornește serverul VPN.
- | 3. Expandați **VPN** → **Conexiuni securizate**.
- | 4. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
- | 5. Faceți clic dreapta pe **CHIGw2MINhost** și selectați **Pornire**.
- | 6. Din meniul **Vizualizare**, selectați **Reîmprospătare**. Dacă conexiunea pornește cu succes, **Starea** se va modifica din *Pornire* sau *La cerere* în *Activată*. Pot trece câteva minute până pornește conexiunea, așa că trebuie să reîmprospătați periodic până când starea se schimbă la *Activată*.

| Testarea conexiunii

| După ce ați terminat de configurat Gateway-B și Gateway-E și ați pornit cu succes serverele VPN, testați conectivitatea pentru a vă asigura că ambele sisteme pot comunica unul cu celălalt. Pentru aceasta, parcurgeți pașii următori:

- | 1. Găsiți un sistem din rețeaua cu PC-A și deschideți o sesiune Telnet.
- | 2. Specificați adresa IP publică pentru Sistem-E, care este 146.210.18.51.
- | 3. Specificați orice informație de logare, dacă este necesară. Dacă puteți vedea ecranul de logare atunci conexiunea funcționează.

Scenariu: Folosirea translatării adreselor de rețea pentru VPN

În acest scenariu, compania dumneavoastră vrea să schimbe date confidențiale cu unul dintre partenerii ei de afaceri utilizând VPN. Pentru a proteja și mai mult structura rețelei, compania dumneavoastră va folosi de asemenea VPN NAT, pentru a ascunde adresa IP privată a sistemului pe care îl folosește pentru a găzdui aplicațiile la care are acces partenerul de afaceri.

Situație

Să presupunem că dumneavoastră sunteți administratorul de rețea 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 și cantități exact atunci când are nevoie de ele, astfel încât furnizorul trebuie să cunoască

starea inventarului companiei dumneavoastră și de planificarea producției. În prezent, efectuați această interacțiune manual, dar constatați că este mare consumatoare de timp, implică un cost ridicat și uneori apar date eronate, astfel încât sunteți mai mult decât doritor să investigați opțiunile pe care le aveți.

Data fiind natura confidențială și dependentă de timp a informațiilor pe care le schimbați, vă decideți să creați o rețea privată virtuală (VPN) între rețeaua furnizorului dumneavoastră și rețeaua companiei dumneavoastră. Pentru a proteja și mai mult confidențialitatea structurii rețelei companiei dumneavoastră, decideți că este nevoie să ascundeți adresa IP privată a sistemului care găzduiește aplicațiile la care furnizorul are acces.

Puteți folosi VPN nu numai pentru a crea definițiile conexiunilor pe gateway-ul VPN din rețeaua companiei dumneavoastră, ci și pentru a furniza translatarea de adrese de care aveți nevoie pentru a ascunde adresele dumneavoastră locale private. Spre deosebire de translatarea adreselor de rețea (network address translation - NAT) convențională, care modifică adresele IP din asocierile de securitate (security associations - SAs) de care are nevoie VPN pentru a funcționa, VPN NAT efectuează translatarea adreselor înainte de validarea SA, prin atribuirea unei adrese conexiunii în momentul în care aceasta este pornită.

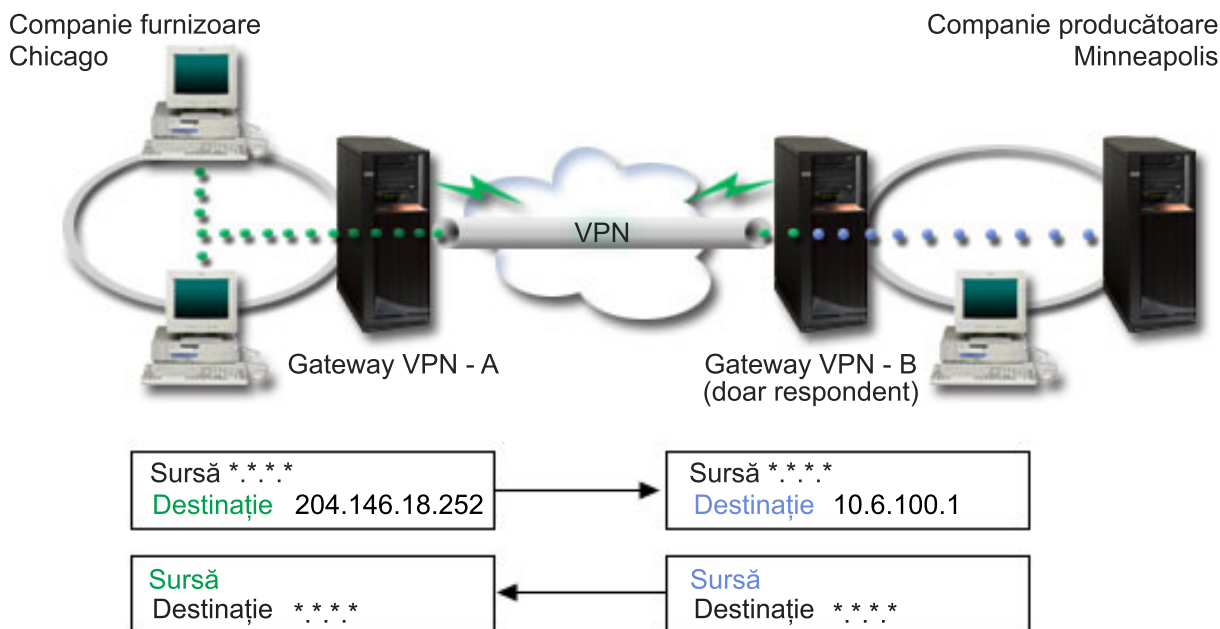
Obiective

Obiectivele acestui scenariu sunt:

- să se permită tuturor clienților din rețeaua furnizorului să acceseze un singur sistem gazdă din rețeaua producătorului printr-o conexiune VPN gateway-la-gateway.
- să se ascundă adresa IP privată a sistemului gazdă din rețeaua producătorului, prin translatarea acesteia într-o adresă IP publică folosind translatarea adreselor de rețea pentru VPN (VPN NAT).

Detalii

Următoarea diagramă ilustrează caracteristicile rețelei atât pentru rețeaua furnizorului, cât și pentru rețeaua producătorului:



- VPN gateway-A este configurat pentru a iniția întotdeauna conexiuni cu VPN gateway-B.
- VPN gateway-A definește capătul destinație pentru conexiune ca 204.146.18.252 (adresa publică atribuită lui iSeries-C).
- iSeries-C are adresa IP privată 10.6.100.1 în rețeaua 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 ieșire, din 10.6.100.1 înapoi în adresa publică a iSeries-C, 204.146.18.252. Din punctul de vedere al clienților din rețeaua furnizorului, iSeries-C are o adresă IP de 204.146.18.252. Ei nu își vor da seama că s-a produs o traducere a adresei.

Task-urile de configurare

Trebuie să efectuați fiecare dintre următoarele task-uri pentru a configura conexiunea descrisă în acest scenariu:

1. Configurați un VPN gateway-la-gateway între **VPN gateway-A** și **VPN gateway-B**.
2. Definiți 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. Configurați **VPN gateway-B** pentru a traduce adresele locale folosind adresele din pool-ul de serviciu local.

Concepte înrudite

“Traducerea adreselor de rețea pentru VPN” la pagina 9

VPN furnizează un mijloc pentru efectuarea de traducere a adreselor de rețea, denumit VPN NAT. VPN NAT diferă de NAT tradițional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE și IPSec.

Studiați acest subiect pentru a afla mai multe.

Planificarea pentru VPN

Primul pas în utilizarea cu succes a VPN-ului este planificarea. Acest subiect furnizează informații despre migrarea de la edițiile anterioare, cerințele de setare și legături către un consilier de planificare care va genera o foaie de lucru personalizată pentru specificațiile dumneavoastră.

Planificarea este o parte esențială a soluției dumneavoastră VPN totale. Sunt multe decizii complexe pe care trebuie să le luați pentru a vă asigura funcționarea corespunzătoare a conexiunii dumneavoastră. Folosiți aceste resurse pentru a aduna toate informațiile de care aveți nevoie pentru a asigura succesul VPN-ului dumneavoastră:

- Cerințele pentru setarea VPN
- Determinarea tipului de VPN ce urmează să fie creat
- Folosirea consilierului de planificare VPN

Consilierul de planificare vă pune întrebări despre rețeaua dumneavoastră și, pe baza răspunsurilor dumneavoastră, vă furnizează sugestii pentru crearea VPN-ului dumneavoastră.

Notă: Folosiți consilierul de planificare VPN doar pentru conexiunile care suportă protocolul Internet Key Exchange (IKE). Pentru conexiunile dumneavoastră manuale, folosiți foaia de lucru pentru planificarea conexiunilor manuale.

- Completarea foilor de lucru pentru planificarea VPN-ului

După ce ați găsit un plan pentru VPN, puteți începe configurarea.

Operații înrudite

Folosirea consilierului de planificare VPN

“Configurarea VPN-ului” la pagina 40

După planificarea pentru VPN, puteți începe configurarea. Acest subiect vă oferă o prezentare generală a ceea ce puteți face cu VPN și în ce fel.

Cerințele pentru setarea VPN

Folosiți aceste informații pentru a vă asigura că îndepliniți cerințele minime pentru crearea unei conexiuni VPN.

Pentru a funcționa corespunzător pe iSeries și cu clienții rețea, asigurați-vă că sistemul și clientul PC îndeplinesc următoarele cerințe:

Cerințe sistem

- OS/400 Versiunea 5 Ediția 2 (5722-SS1) sau mai recentă
- Digital Certificate Manager (5722-SS1 opțiunea 34)
- iSeries Access pentru Windows (5722-XE1)
- Navigator iSeries
 - Componenta Rețea din Navigator iSeries
- Setări valoarea sistem reținere date de securitate de pe server (QRETSVRSEC *SEC) la 1.
- TCP/IP trebuie să fie configurat, inclusiv interfețe IP, rute, nume gazdă locală și nume domeniu local.

Cerințe client

- O stație de lucru cu un sistem de operare Windows pe 32 de biți, conectată corespunzător la sistemul dumneavoastră și configurată pentru TCP/IP
- O unitate de procesare la 233 MHz
- 32 MB RAM pentru clienții Windows pentru Windows 95
- 64 MB RAM pentru clienții Windows NT 4.0 și Windows 2000
- iSeries Access pentru Windows și Navigator iSeries instalate pe PC-ul client
- Software care suportă protocolul IP Security (IPSec)
- Software care suportă L2TP, dacă utilizatorii de la distanță vor folosi L2TP pentru a stabili o conexiune cu sistemul dumneavoastră.

Operații înrudite

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Determinarea tipului de VPN ce urmează să fie creat

Aceste informații vă pot ajuta să decideți asupra diverselor tipuri de conexiune pe care le puteți seta.

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

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

Gateway-la-gateway

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

Gateway-la-gazdă

IPSec protejează traficul de date ce călătorește între un gateway și un calculator gazdă dintr-o rețea la distanță. VPN nu protejează traficul de date din rețeaua locală deoarece este considerat de încredere.

Gazdă-la-gateway

VPN protejează traficul de date care călătorește între un calculator gazdă din rețeaua locală și un gateway la distanță. VPN nu protejează traficul de date din rețeaua la distanță.

Gazdă-la-gazdă

Capetele conexiunii sunt aceleași cu capetele datelor pe ambele sisteme (local și la distanță). VPN protejează traficul de date care călătorește între un calculator gazdă din rețeaua locală și un calculator gazdă din rețeaua la distanță. Acest tip de VPN furnizează protecție IPSec end-to-end.

Completarea foilor de lucru pentru planificarea VPN-ului

Folosiți foile de lucru pentru planificarea VPN pentru a culege informații detaliate privind planurile de folosire a VPN-ului. Aveți nevoie de aceste informații pentru a vă planifica în mod adecvat strategia VPN. De asemenea, puteți folosi aceste informații pentru a vă configura VPN-ul.

Dacă preferați, puteți tipări și completa foile de lucru pentru planificare, pentru a culege informații detaliate privind planurile de folosire a VPN-ului.

Alegeți foaia de lucru pentru tipul de conexiune pe care doriți să-l creați.

- Foaia de lucru pentru planificarea conexiunilor dinamice
- Foaia de lucru pentru planificarea conexiunilor
- Consilier planificare VPN

Sau, dacă preferați, folosiți consilierul pentru planificare interactivă și pentru îndrumare la configurare. Consilierul de planificare vă pune întrebări despre rețeaua dumneavoastră și, pe baza răspunsurilor dumneavoastră, vă furnizează sugestii pentru crearea VPN-ului dumneavoastră.

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

Dacă veți crea conexiuni multiple cu proprietăți similare, poate doriți să setați valorile implicite VPN. Valorile implicite pe care le configurați furnizează informațiile din foile de proprietăți VPN. Aceasta înseamnă că nu e necesar să configurați aceleași proprietăți de mai multe ori. Pentru a seta valorile implicite VPN, selectați **Editare** din meniul principal VPN, și apoi selectați **Implicite**.

Informații înrudite

Consilier planificare VPN

Foaia de lucru pentru planificarea conexiunilor dinamice

Completați această foaie de lucru înainte de a configura o conexiune dinamică.

Înainte de a vă crea conexiunile VPN dinamice, completați această foaie de lucru. Foaia de lucru presupune că veți folosi vrăjitorul de Conexiune nouă. Vrăjitorul vă permite să setați un VPN pe baza cerințelor dumneavoastră primare de securitate. În anumite cazuri, poate fi nevoie să rafinați proprietățile pe care vrăjitorul le configurează pentru o conexiune. De exemplu, puteți decide dacă doriți jurnalizare sau dacă doriți ca serverul VPN să pornească de fiecare dată când pornește TCP/IP. În acest caz, faceți clic dreapta pe grupul sau conexiunea de grup dinamic creată de vrăjitor și selectați **Proprietăți**.

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

Tabela 8. Cerințele sistemului

| Listă de verificare pentru cerințele preliminare | Răspunsuri |
|---|------------|
| Sistemul dumneavoastră de operare este OS/400 V5R2 (5722-SS1) sau ulterior? | Da |
| Este instalat Digital Certificate Manager (5722-SS1 opțiunea 34)? | Da |
| Este instalat iSeries Access pentru Windows (5722-XE1)? | Da |
| Este instalat Navigator iSeries? | Da |
| Este instalată subcomponenta Rețea din Navigator iSeries? | Da |
| Este instalat TCP/IP Connectivity Utilities (5722-TC1)? | Da |

Tabela 8. Cerințele sistemului (continuare)

| Listă de verificare pentru cerințele preliminare | Răspunsuri |
|--|------------|
| Ați setat la 1 valoarea de sistem pentru reținerea datelor de securitate ale serverului (QRETSVRSEC *SEC)? | Da |
| Este configurat TCP/IP pe sistem (inclusiv interfețele IP, rutele, numele de gazdă locală și numele de domeniu local)? | Da |
| Este stabilită comunicația TCP/IP normală între punctele finale cerute? | Da |
| Ați aplicat cele mai recente corecții 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 și ESP? | Da |
| Sunt configurate firewall-urile sau ruterul pentru a permite protocoalele IKE (UDP port 500), AH și ESP? | Da |
| Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP? | Da |

Tabela 9. Configurația VPN

| Aveți nevoie de aceste informații pentru a configura o conexiune dinamică VPN | Răspunsuri |
|---|------------|
| Ce tip de conexiune creați? <ul style="list-style-type: none"> • Gateway-la-gateway • Gazdă-la-gateway • Gateway-la-gazdă • Gazdă-la-gazdă | |
| Cum veți denumi grupul de chei dinamice? | |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? <ul style="list-style-type: none"> • Cea mai bună securitate, cele mai mici performanțe • Echilibrarea securității cu performanța • Cea mai joasă securitate și cea mai bună performanță | |
| Folosiți certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată? | |
| Care este identificatorul serverului de chei local? | |
| Care este identificatorul serverului de chei local? | |
| Care este identificatorul serverului de chei la distanță ? | |
| Care este identificatorul punctului final de date la distanță ? | |
| De ce tip de securitate și performanțe ale sistemului aveți nevoie pentru a vă proteja cheile? <ul style="list-style-type: none"> • Cea mai bună securitate, cele mai mici performanțe • Echilibrarea securității cu performanța • Cea mai joasă securitate și cea mai bună performanță | |

Foaia de lucru pentru planificarea conexiunilor

Completați această foaie de lucru înainte de a vă configura o conexiune manuală.

Completați acest tabel pentru a vă ajuta la crearea conexiunilor rețelei dumneavoastră private (VPN) care nu folosesc IKE pentru gestiune cheilor. Răspundeți la fiecare din aceste întrebări înainte de a continua cu setarea VPN:

Tabela 10. Cerințe sistem

| Listă de verificare cerințe preliminare | Răspunsuri |
|---|------------|
| Sistemul dumneavoastră de operare este OS/400 V5R2 (5722-SS1) sau ulterior? | |
| Este instalat Digital Certificate Manager (5722-SS1 opțiunea 34)? | |

Tabela 10. Cerințe sistem (continuare)

| | |
|--|--|
| Este instalat iSeries Access pentru Windows (5722-XE1)? | |
| Este instalat Navigator iSeries? | |
| Este instalată subcomponenta Rețea din Navigator iSeries? | |
| Este instalat TCP/IP Connectivity Utilities (5722-TC1)? | |
| Ați setat la 1 valoarea de sistem pentru reținerea datelor de securitate ale serverului (QRETSVRSEC *SEC)? | |
| Este configurat TCP/IP pe sistem (inclusiv interfețele IP, rutele, numele de gazdă locală și numele de domeniu local)? | |
| Este stabilită comunicația TCP/IP normală între punctele finale cerute? | |
| Ați aplicat cele mai recente corecții temporare de program (PTF-uri)? | |
| 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 și ESP? | |
| Sunt configurate firewall-urile sau ruterul pentru a permite protocoalele AH și ESP? | |
| Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP? | |

Tabela 11. Configurația VPN

| Aveți nevoie de aceste informații pentru a configura manual un VPN | Răspunsuri |
|--|------------|
| Ce tip de conexiune creați? • Gazdă-la-gazdă • Gazdă-la-gateway • Gateway-la-gazdă • Gateway-la-gateway | |
| Cum veți denumi conexiunea? | |
| Care este identificatorul capătului local al conexiunii? | |
| Care este identificatorul capătului la distanță al conexiunii? | |
| Care este identificatorul punctului final de date local ? | |
| Care este identificatorul punctului final de date la distanță ? | |
| Ce tip de trafic veți permite pentru această conexiune (port local, port la distanță și protocol)? | |
| Aveți nevoie de traducere de adrese pentru această conexiune? Consultați Traducerea adreselor de rețea pentru VPN pentru informații suplimentare. | |
| Veți folosi modul tunel sau modul transport? | |
| Ce protocol IPSec va folosi conexiunea (AH, ESP sau AH cu ESP)? Consultați Securitate IP (IPSec) pentru informații suplimentare. | |
| Ce algoritm de autentificare va folosi conexiunea (HMAC-MD5 sau HMAC-SHA)? | |
| Ce algoritm de criptare va folosi conexiunea (DES-CBC sau 3DES-CBC)? Notă: Specificați un algoritm de criptare numai dacă ați selectat ESP ca protocol IPSec. | |
| Care este cheia de intrare AH? Dacă folosiți MD5, cheia este un șir hexazecimal de 16 octeți. Dacă folosiți SHA, cheia este un șir hexazecimal de 20 de octeți. Cheia dumneavoastră de intrare trebuie să corespundă exact cheii de ieșire a serverului de la distanță. | |
| Care este cheia de ieșire AH? Dacă folosiți MD5, cheia este un șir hexazecimal de 16 octeți. Dacă folosiți SHA, cheia este un șir hexazecimal de 20 de octeți. Cheia dumneavoastră de ieșire trebuie să corespundă exact cheii de intrarea serverului de la distanță. | |

Tabela 11. Configurația VPN (continuare)

| | |
|--|--|
| Care este cheia de intrare ESP? Dacă folosiți DES, cheia este un șir hexazecimal de 8 octeți. Dacă folosiți 3DES, cheia este un șir hexazecimal de 24 de octeți. | |
| Cheia dumneavoastră de intrare trebuie să corespundă exact cheii de ieșire a serverului de la distanță. | |
| Care este cheia de ieșire ESP? Dacă folosiți DES, cheia este un șir hexazecimal de 8 octeți. Dacă folosiți 3DES, cheia este un șir hexazecimal de 24 de octeți. | |
| Cheia dumneavoastră de ieșire trebuie să corespundă exact cheii de intrarea serverului de la distanță. | |
| Care este Indexul politicii de securitate de intrare (SPI)? SPI de intrare este un șir hexazecimal de 4 octeți, unde primul octet este setat la 00. | |
| SPI-ul dumneavoastră de intrare trebuie să corespundă exact cu SPI-ul de ieșire al serverului de la distanță. | |
| Care este SPI-ul de ieșire? SPI de ieșire este un șir hexazecimal de 4 octeți. | |
| SPI-ul dumneavoastră de ieșire trebuie să corespundă exact cu SPI-ul de intrare al serverului de la distanță. | |

Concepte înrudite

“Traducerea adreselor de rețea pentru VPN” la pagina 9

VPN furnizează un mijloc pentru efectuarea de traducere a adreselor de rețea, denumit VPN NAT. VPN NAT diferă de NAT tradițional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE și IPSec.

Studiați acest subiect pentru a afla mai multe.

Configurarea VPN-ului

După planificarea pentru VPN, puteți începe configurarea. Acest subiect vă oferă o prezentare generală a ceea ce puteți face cu VPN și în ce fel.

Interfața VPN vă furnizează câteva moduri diferite de configurare a conexiunilor dumneavoastră VPN. Continuați să citiți pentru a vă putea decide ce tip de conexiune vreți să configurați și cum să o faceți.

Concepte înrudite

“Planificarea pentru VPN” la pagina 35

Primul pas în utilizarea cu succes a VPN-ului este planificarea. Acest subiect furnizează informații despre migrarea de la edițiile anterioare, cerințele de setare și legături către un consilier de planificare care va genera o foaie de lucru personalizată pentru specificațiile dumneavoastră.

Ce tip de conexiune ar trebui să configurez?

O conexiune dinamică este una care generează și 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 consecință, este puțin probabil că un atacator poate să captureze o cheie, să aibă timp să o spargă, și să o folosească la dirijarea sau capturarea traficului pe care cheia îl protejează.

O conexiune manuală, totuși, nu furnizează suport pentru negocierile IKE și în consecință pentru gestiunea automată a cheilor. Mai departe, amândouă terminările de conexiune necesită să le configurați diferite atribute care trebuie să se potrivească exact. Conexiunile manuale folosesc chei statice care nu se reînprospătează sau schimbă atâta timp cât conexiunea este activă. Trebuie să opriți o conexiune manuală pentru a schimba cheile sale asociate. În cazul în care considerați aceasta un risc de securitate, puteți vrea să creați 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 funcționeze corect. Urmați legăturile de mai jos pentru informații specifice despre cum să configurați fiecare dintre obiectele de configurare VPN:

Indiciu: Configurarea conexiunilor vrăjitorul de Conexiune nouă

În general, puteți utiliza vrăjitorul Conexiune pentru a crea toate conexiunile dumneavoastră dinamice. Vrăjitorul creează automat fiecare obiect de configurație de care VPN are nevoie pentru a funcționa corespunzător, inclusiv regulile de pachete. Dacă specificați că vreți ca vrăjitorul să activeze regulile de pachete VPN pentru dumneavoastră, puteți trece peste pasul 6 de mai jos, *Pornirea conexiunii*. Altfel, după ce vrăjitorul termină configurarea VPN-ului, trebuie să activați regulile de pachete și apoi puteți porni conexiunea.

Dacă alegeți să nu folosiți vrăjitorul pentru a configura conexiunile VPN dinamice, urmați acești pași pentru a completa configurația:

1. Configurați politicile de securitate VPN

Trebuie să definiți politicile de securitate VPN pentru toate conexiunile dumneavoastră dinamice. Politica Internet Key Exchange și politica de date dictează cum IKE își protejează negocierile din faza 1 și faza 2.

2. Configurarea conexiunilor securizate

După ce ați definit politicile de securitate pentru o conexiune, trebuie să configurați conexiunea securizată. Pentru conexiunile dinamice, obiectul de conexiune securizată include un grup de chei dinamice și o conexiune de chei dinamice. **Grupul de chei dinamice** definește caracteristicile comune ale uneia sau mai multe conexiuni VPN, în timp ce **conexiunea de chei dinamice** definește caracteristicile conexiunilor de date individuale între perechi de puncte finale. Conexiunea de chei dinamice există în grupul de chei dinamice.

Notă: Puteți completa doar următorii doi pași, *Configurarea de reguli pachete* și *Definirea unei interfețe pentru reguli*, dacă selectați opțiunea **Regula de filtru politici va fi definită în regulile pachete** de la pagina **Grup de chei dinamice - Conexiuni** din interfața VPN. Altfel, aceste reguli sunt create ca parte din configurațiile dumneavoastră VPN și sunt aplicate la interfața pe care o specificați.

Este recomandat să permiteți întotdeauna ca interfața VPN să vă creeze regulile de filtrare a politicii. Faceți aceasta selectând opțiunea **Generare filtru următor de politică pentru acest grup** în pagina **Grup de chei dinamice - Conexiuni**.

3. Configurarea de reguli pachete

După ce terminați configurarea VPN, trebuie să creați și să aplicați reguli de filtrare care permit traficului de date să traverseze conexiunea. Regulile VPN **pre-IPSec** permit întregului trafic IKE pe interfețele specificate astfel încât IKE poate negocia conexiuni. Regula **filtru de politică** definește care adrese, protocoale și porturi pot folosi grupul nou de chei dinamice asociat.

Dacă migrați de la V4R4 sau V4R5 și aveți conexiuni VPN și filtre de politică pe care vreți să continuați să le utilizați în ediția curentă, revedeți subiectul, *Migrare filtre de politică în ediția curentă* pentru a vă asigura că filtrele de politică vechi și cele noi vor lucra împreună așa cum intenționați dumneavoastră.

4. Definirea unei interfețe pentru reguli

După ce ați configurat regulile de pachete și orice altă regulă care aveți nevoie să activeze conexiunea dumneavoastră VPN, ar trebui să definiți o interfață pe care să le aplicați.

5. Activarea de reguli pachete

După ce ați definit o interfață pentru regulile dumneavoastră de pachete, trebuie să le activați înainte să puteți porni conexiunea.

6. Pornirea conexiunii

Finalizați această operație pentru a porni conexiunile.

Cum configurez o conexiune VPN manual?

După cum sugerează și numele, o conexiune manuală este una unde trebuie să configurați toate proprietățile dumneavoastră VPN manual, inclusiv cheile de intrare și ieșire. Uurmați legăturile de mai jos pentru informații specifice despre cum să configurați o conexiune manuală:

1. Configurarea de conexiuni manual

Conexiunile manuale definesc caracteristicile unei conexiuni inclusiv tipul de protocoale de securitate, conexiunea și punctele finale de date.

Notă: Trebuie doar să efectuați următorii doi pași, *Configurarea regulii de filtrare politici și Definierea unei interfețe pentru reguli*, dacă selectați opțiunea **Regula de filtrare politici va fi definită în regulile de pachete** de la pagina **Conexiune manuală - Conexiune** în interfața VPN. Altfel, aceste reguli sunt create ca parte din configurațiile dumneavoastră VPN.

Este recomandat să permiteți întotdeauna ca interfața VPN să vă creeze regulile de filtrare a politicii. Faceți aceasta selectând opțiunea **Generare filtru de politică potrivit cu punctele finale de date**, în pagina **Conexiune manuală - Conexiune**.

2. Configurarea regulii de filtrare politici

După ce configurați atributele conexiunii manuale, trebuie să creați și să aplicați o regulă de filtrare politici care să permită traficului de date să traverseze conexiunea. Regula de **filtrare politici** definește care adrese, protocoale și porturi pot folosi conexiunea asociată.

3. Definierea unei interfețe pentru reguli

După ce ați configurat regulile de pachete și orice altă regulă care aveți nevoie să activeze conexiunea dumneavoastră VPN, ar trebui să definiți o interfață pe care să le aplicați.

4. Activarea regulilor de pachete

După ce ați definit o interfață pentru regulile dumneavoastră de pachete, trebuie să le activați înainte să puteți porni conexiunea.

5. Pornirea conexiunii

Finalizați această operație pentru a porni conexiunile care sunt inițiate local.

Configurarea conexiunilor VPN cu vrăjitorul Conexiune nouă

Vrăjitorul de conexiune nouă vă permite să creați o rețea privată virtuală (VPN) între orice combinație de gazdă și gateway.

De exemplu, gazdă-la-gazdă, gateway-la-gazdă, gazdă-la-gateway sau gateway-la-gateway.

Vrăjitorul creează automat fiecare obiect de configurație de care VPN are nevoie pentru a funcționa corespunzător, inclusiv regulile de pachete. Totuși, dacă aveți nevoie să adăugați funcții la VPN, de exemplu jurnalizare sau translatarea adreselor de rețea pentru VPN (VPN NAT), ați putea să vă rafinați VPN prin tabelele de proprietăți ale grupurilor de chei dinamice sau conexiunilor corespunzătoare. Pentru aceasta, trebuie să opriți întâi conexiunea dacă este activă. Apoi faceți clic dreapta pe grupul de chei dinamice sau conexiune și selectați **Proprietăți**.

Completați Consilierul de planificare VPN înainte de a începe. Consilierul vă furnizează un mijloc de a aduna informații importante de care aveți nevoie pentru a crea VPN.

Pentru a crea un VPN cu vrăjitorul de conexiune, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Rețea privată virtuală** și selectați **Conexiune nouă** pentru a porni vrăjitorul.
3. Finalizați vrăjitorul pentru a crea o conexiune VPN de bază. Faceți clic pe **Ajutor**, dacă aveți nevoie de ajutor.

Operații înrudite

Consilier planificare VPN

Configurați politicile de securitate VPN

După ce determinați cum veți folosi VPN-ul, trebuie să vă definiți politicile de securitate pentru VPN.

Notă: După ce configurați politicile de securitate VPN, trebuie apoi să configurați conexiunile securizate.

Operații înrudite

“Configurarea conexiunilor sigure VPN” la pagina 44

După ce ați configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configurați conexiunea sigură.

Configurarea unei politici IKE (Internet Key Exchange)

Politica IKE definește ce nivel de autentificare și protecție prin criptare folosește IKE în timpul fazei 1 a negocierilor.

Faza 1 IKE stabilește cheile care protejează mesajele care se transmit în negocierile următoare din faza 2. Nu este nevoie să definiți o politică IKE când creați o conexiune manuală. În plus, dacă vă creați VPN-ul cu vrăjitorul Conexiune nouă, acesta poate crea politica IKE în locul dumneavoastră.

VPN folosește fie modul semnătură RSA, fie chei prepartajate pentru a autentifica negocierile de fază 1. Dacă aveți de gând să folosiți certificate digitale pentru autentificarea serverelor de chei, trebuie întâi să le configurați folosind Digital Certificate Manager (5722-SS1 opțiunea 34). Politica IKE de asemenea identifică ce server de chei la distanță va folosi această politică.

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

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Politici de securitate IP**.
2. Pentru a crea o nouă politică, faceți clic dreapta pe **Politici Internet Key Exchange** și selectați **Politică nouă Internet Key Exchange**. Pentru a face modificări la o politică existentă, apăsați pe **Politici Internet Key Exchange** în panoul stâng, apoi faceți clic dreapta pe politica de date pe care vreți să o modificați în panoul drept și selectați **Proprietăți**.
3. Completați fiecare tabel de proprietăți. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** pentru a salva modificările.

Se recomandă să utilizați 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 utilizați chei prepartajate și negocierea mod agresiv, selectați parole pentru care este puțin probabil să fie sparte în atacurile care scanează dicționarul. Se recomandă de asemenea să vă modificați periodic parolele. Pentru a forța un schimb de chei să utilizeze negocierea în mod principal, executați următoarele operații:

1. În Navigator iSeries, expandați serverul **Rețea** → **Politici IP**.
2. Selectați **VPN** → **Politici de securitate IP** → **Politici Internet Key Exchange** pentru a vedea politicile de schimb chei definite curent în panoul din dreapta.
3. Faceți clic dreapta pe o anumită politică de schimb de chei și selectați **Proprietăți**.
4. În pagina Transformare, faceți clic pe **Politică răspuns**. Apare dialogul Politică Internet Key Exchange respondent.
5. În câmpul Protecție identitate, deselectați **Negociere în mod agresiv IKE (fără protecție identitate)**.
6. Faceți clic pe **OK** pentru a vă întoarce în dialogul Proprietăți.
7. Apăsați **OK** din nou pentru a salva modificările.

Notă: Când setați câmpul protecție identitate, modificarea se aplică pentru toate schimburile cu servere cheie la distanță, deoarece există doar o politică IKE de răspuns pentru întregul sistem. Negocierea mod principal asigură că sistemul de inițiere poate doar cere un schimb de politică cheie mod principal.

Concepte înrudite

“Gestionarea cheilor” la pagina 6

Un VPN dinamic furnizează securitate suplimentară pentru comunicațiile 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.

Operații înrudite

Digital Certificate Manager

Configurarea unei politici de date

O politică de date definește 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 definiți o politică de date când creați o conexiune manuală. În plus, dacă vă creați VPN-ul cu vrăjitorul Conexiune nouă, acesta poate crea politica de date în locul dumneavoastră.

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

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Politici de securitate IP**.
2. Pentru a crea o nouă politică de date, faceți clic dreapta pe **Politici de date** și selectați **Politică de date nouă**. Pentru a face modificări la o politică de date existentă, apăsați pe **Politici de date** (în panoul stâng) apoi faceți clic dreapta pe politica de date pe care vreți să o modificați (în panoul drept) și selectați **Proprietăți**.
3. Completați fiecare tabel de proprietăți. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** pentru a salva modificările.

Concepte înrudite

“Gestionarea cheilor” la pagina 6

Un VPN dinamic furnizează securitate suplimentară pentru comunicațiile 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.

Configurarea conexiunilor sigure VPN

După ce ați configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configurați conexiunea sigură.

Pentru conexiunile dinamice, obiectul de conexiune securizată include un grup de chei dinamice și o conexiune de chei dinamice.

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

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

Pentru a configura obiectul conexiune securizată, executați atât task-urile din Partea întâi, cât și cele din Partea a doua.

Concepte înrudite

“Configurați politicile de securitate VPN” la pagina 43

După ce determinați cum veți folosi VPN-ul, trebuie să vă definiți politicile de securitate pentru VPN.

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Operații înrudite

“Activarea regulilor pachet VPN” la pagina 50

Trebuie să activați regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Partea întâi: Configurarea unui grup de chei dinamice

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Faceți clic dreapta pe **După grup** și selectați **Grup nou de chei dinamice**.
3. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** pentru a salva modificările.

Partea a doua: Configurarea unei conexiuni chei dinamice

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate** → **După grup**.
2. În panoul din stânga al ferestrei Navigator iSeries, faceți clic dreapta pe grupul de chei dinamice pe care l-ați creat în partea întâi și selectați **Conexiune nouă de chei dinamice**.
3. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** pentru a salva modificările.

După ce ați făcut acești pași, trebuie să activați regulile pachet pe care le cere conexiunea pentru a funcționa corespunzător.

Notă: În majoritatea cazurilor, permiteți interfeței VPN să genereze reguli pachet VPN automat prin selectarea opțiunii **Generare următorul filtru politică pentru acest grup** în pagina **Grup cheie dinamică - Conexiuni**. Însă dacă selectați opțiunea **Filtrul de politici va fi definit în Reguli pachet**, atunci trebuie să configurați reguli de filtrare VPN folosind editorul Reguli pachet și apoi să le activați.

Configurarea unei conexiuni manuale

Așa cum sugerează numele, o conexiune manuală este una în care trebuie să configurați toate proprietățile VPN de mână.

Mai mult, ambele capete ale conexiunii vă cer să configurați câteva elemente care trebui să se potrivească *exact*. De exemplu, cheile dumneavoastră de intrare trebuie să se potrivească cu cheile de ieșire ale sistemului de la distanță, altfel conexiunea va eșua.

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

Pentru a defini proprietățile conexiunii dumneavoastră manuale, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → → **Conexiuni securizate**.
2. Faceți clic dreapta pe **Toate conexiunile** și selectați **Conexiune manuală nouă**.
3. Completați fiecare tabel de proprietăți. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** pentru a salva modificările.

Notă: În majoritatea cazurilor, permiteți interfeței VPN să genereze reguli pachet VPN automat prin selectarea opțiunii **Generare filtru politică care se potrivește cu punctele finale de date** în pagina **Conexiune manuală - conexiune**. Totuși, dacă selectați opțiunea **Filtrul de politică va fi definit în Reguli pachet**, atunci trebuie să configurați o regulă de filtrare a politicii manual și apoi să o activați.

Operații înrudite

“Configurarea unei reguli filtrare politici” la pagina 48

Folosiți aceste informații pentru a afla cum să editați regulile de filtrare politici.

Configurarea regulilor de pachete VPN

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Dacă decideți să creați regulile pachet VPN utilizând editorul Reguli pachet din Navigator iSeries, creați și alte reguli suplimentare în același fel. Invers, dacă lăsați VPN-ul să vă genereze regulile filtru politică, creați toate regulile filtru politică suplimentare în acest mod.

În general, VPN cere două tipuri de reguli de filtrare: reguli de filtrare Pre-IPSec și reguli de filtrare de politici. Revedeți subiectele de mai jos pentru a afla cum se configurează aceste reguli folosind editorul de reguli de pachete din Navigator iSeries. Dacă vreți să citiți despre alte opțiuni VPN și de filtrare, vedeți secțiunea Filtrare VPN și IP din subiectul concepte VPN.

- Configurarea regulii de filtrare pre-IPSec

Regulile pre-IPSec sunt orice reguli care din sistem care vin înainte de regulile cu un tip de acțiune IPSEC. Acest subiect discută doar despre regulile pre-IPSec cerute de VPN pentru a funcționa corespunzător. În acest caz, regulile pre-IPSec sunt o pereche de reguli care permit procesarea IKE peste conexiune. IKE permite ca generarea și negocierea dinamică de chei să aibă loc pe conexiunea dumneavoastră. Ați putea avea nevoie să adăugați alte reguli pre-IPSec, depinzând de mediul particular de rețea și de politica de securitate.

Notă: Trebuie să configurați acest tip de regulă pre-IPSec doar dacă aveți 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.

- Configurarea unei reguli filtrare politici

Regula de filtrare politică definește traficul care poate folosi VPN și ce politică de protecție a datelor să se aplice acestui trafic.

Lucruri de luat în seamă înainte de a începe

Când adăugați reguli de filtrare pentru a interfață, sistemul adaugă automat o regulă implicită de negare pentru acea interfață. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteți și nu puteți schimba această regulă. Ca rezultat, puteți vedea că trafic care înainte trecea, în mod misterios nu mai funcționează după ce activați regulile de filtrare VPN. Dacă doriți să permiteți alt trafic decât VPN prin interfață, trebuie să adăugați reguli explicite de permitere.

După ce configurați regulile de filtrare corespunzătoare, trebuie să definiți interfața la care ele se aplică, apoi să le activați.

Este esențial să vă configurați regulile de filtrare corespunzător. Altfel, regulile de filtrare pot bloca tot traficul IP care vine și pleacă din sistem. Aceasta include și conexiunea cu Navigator iSeries, pe care o folosiți pentru a configura regulile de filtrare.

Dacă regulile de filtrare nu permit traficul pentru Navigator iSeries, Navigator iSeries nu poate comunica cu sistemul. Dacă vă găsiți în această situație, trebuie să vă logați la sistem utilizând o interfață care are încă conectivitate, cum ar fi consola de operații. Folosiți comanda RMVTCPTBL pentru a înlătura toate filtrele din sistem. Această comandă de asemenea oprește toate serverele *VPN apoi le pornește din nou. Apoi configurați filtrele și reactivați-le.

Concepte înrudite

“VPN și filtrarea IP” la pagina 12

Filtrarea IP și VPN sunt foarte înrudite. De fapt, majoritatea conexiunilor VPN necesită reguli de filtrare pentru a funcționa corect. Acest subiect vă oferă informații despre ce filtre necesită VPN, împreună cu alte concepte de filtrare înrudite cu VPN.

Operații înrudite

“Configurarea conexiunilor sigure VPN” la pagina 44

După ce ați configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configurați conexiunea sigură.

“Configurarea regulii de filtrare pre-IPSec”

Aceste informații vă pot ajuta să creați reguli de filtrare pentru traficul de intrare și de ieșire.

“Configurarea unei reguli filtrare politici” la pagina 48

Folosiți aceste informații pentru a afla cum să editați regulile de filtrare politici.

“Definirea interfeței pentru regulile de filtru VPN” la pagina 49

După ce v-ați configurat regulile pachet VPN și orice alte reguli de care aveți nevoie, pentru a vă activa conexiunea VPN trebuie să definiți interfața la care se aplică.

“Activarea regulilor pachet VPN” la pagina 50

Trebuie să activați regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Configurarea regulii de filtrare pre-IPSec

Aceste informații vă pot ajuta să creați reguli de filtrare pentru traficul de intrare și de ieșire.

Atenție: Efectuați această operație doar dacă ați specificat că nu vreți ca VPN să vă genereze regulile filtrare politică automat.

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

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Reguli pachet** și selectați **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creați sau să editați filtre și reguli NAT pentru sistemul dumneavoastră.
3. În fereastra Bine ați venit, selectați **Creare fișier regulă pachet nou** și faceți clic pe **OK**.
4. Din editorul Reguli pachet selectați **Inserare** → **Filtru**.
5. În pagina **General**, specificați un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puțin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică și unul pentru regulile de filtru PERMIT și DENY. Numiți setul care conține regulile dumneavoastră de filtru pre-IPSec cu prefixul *preipsec*. De exemplu, *preipsecfilters*.
6. În câmpul **Acțiune**, selectați **PERMIT** din lista derulantă.
7. În câmpul **Direcție**, selectați **DE IEȘIRE** din lista derulantă.
8. În câmpul **Nume adresă sursă**, selectați **=** din prima listă derulantă și apoi introduceți adresa IP a serverului local de chei în al doilea câmp. Ați specificat adresa IP a serverului local de chei în politica IKE.
9. În câmpul **Nume adresă destinație**, selectați **=** din prima listă derulantă și apoi introduceți adresa IP a serverului la distanță de chei în al doilea câmp. Ați specificat de asemenea adresa IP a serverului la distanță de chei în politica IKE.
10. În pagina **Servicii**, selectați **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** și **Port destinație**.
11. În câmpul **Protocol**, selectați **UDP** din lista derulantă.
12. Pentru **Portul sursă**, selectați **=** în primul câmp, apoi introduceți 500 în al doilea câmp.
13. Repetați pasul anterior pentru **Portul destinație**.
14. Faceți clic pe **OK**.

15. Repetați acești pași pentru a configura filtrul INBOUND. Folosiți același nume de set și inversați adresele dacă e nevoie.

Notă: O opțiune mai puțin sigură, dar mai ușoară pentru permiterea traficului IKE prin conexiune, este să configurați doar un filtru pre-IPSec și să folosiți înlocuitori de caractere (*) în câmpurile **Direcție**, **Nume adresă sursă** și **Nume adresă destinație**.

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

Concepte înrudite

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Operații înrudite

“Configurarea unei reguli filtrare politici”

Folosiți aceste informații pentru a afla cum să editați regulile de filtrare politici.

Configurarea unei reguli filtrare politici

Folosiți aceste informații pentru a afla cum să editați regulile de filtrare politici.

Atenție: Efectuați acest task doar dacă ați specificat că nu vreți ca VPN să vă genereze regulile de filtrare politici automat.

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

Notă: Dacă doar ați configurat regula pre-IPSec (doar pentru conexiuni dinamice) editorul Reguli pachet va fi încă deschis; deplasați-vă la pasul 4.

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Reguli pachet** și selectați **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creați sau să editați filtre și reguli NAT pentru sistemul dumneavoastră.
3. În fereastra Bine ați venit, selectați **Creare fișier regulă pachet nou** și faceți clic pe **OK**.
4. Din editorul Reguli pachet selectați **Inserare** → **Filtru**.
5. În pagina **General**, specificați un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puțin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică și unul pentru regulile de filtru PERMIT și DENY. De exemplu, **policyfilters**
6. În câmpul **Acțiune**, selectați **IPSEC** din lista derulantă. Câmpul **Direcție** este implicit pe DE IEȘIRE și nu puteți să-l schimbați. Deși acest câmp este implicit pe OUTBOUND, este de fapt bi-direcțional. Apare OUTBOUND pentru a clarifica semantica valorilor de intrare. De exemplu, valorile sursă sunt valori locale și valorile destinație sunt valori la distanță.
7. Pentru **Nume adresă sursă**, selectați **=** în primul câmp și apoi introduceți adresa IP a punctului final local de date în al doilea câmp. Puteți de asemenea să specificați un interval de adrese IP sau o adresă IP plus o mască de subrețea după ce le definiți folosind funcția **Definire Adrese**.
8. Pentru **Nume adresă destinație**, selectați **=** în primul câmp și apoi introduceți adresa IP a punctului final la distanță de date în al doilea câmp. Puteți de asemenea să specificați un interval de adrese IP sau o adresă IP plus o mască de subrețea după ce le definiți folosind funcția **Definire adresă**.
9. În câmpul **Jurnalizare**, specificați ce nivel de jurnalizare aveți nevoie.
10. În câmpul **Nume conexiune**, selectați definiția conexiunii la care se aplică aceste reguli de filtrare.
11. (opțional) Introduceți o descriere.
12. În pagina **Servicii**, selectați **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** și **Port destinație**.

13. În câmpurile **Protocol**, **Port sursă** și **Port destinație**, selectați valoarea corespunzătoare pentru trafic. Sau, puteți selecta asteriscul (*) din lista derulantă. Aceasta permite oricărui protocol care folosește orice port să folosească VPN.
14. Faceți clic pe **OK**.

Următorul pas este să definiți interfața la care se aplică aceste reguli de filtrare.

Notă: Când adăugați reguli de filtrare pentru o interfață, sistemul adaugă automat o regulă implicită de negare pentru acea interfață. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteți și nu puteți schimba această regulă. În consecință, s-ar putea să vedeți că anumite conexiuni care au funcționat anterior eșuează misterios după ce vă activați regulile pachet VPN. Dacă doriți să permiteți alt trafic decât VPN prin interfață, trebuie să adăugați reguli explicite de permitere.

Concepte înrudite

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Operații înrudite

“Configurarea unei conexiuni manuale” la pagina 45

Așa cum sugerează numele, o conexiune manuală este una în care trebuie să configurați toate proprietățile VPN de mână.

“Configurarea regulii de filtrare pre-IPSec” la pagina 47

Aceste informații vă pot ajuta să creați reguli de filtrare pentru traficul de intrare și de ieșire.

“Definirea interfeței pentru regulile de filtru VPN”

După ce v-ați configurat regulile pachet VPN și orice alte reguli de care aveți nevoie, pentru a vă activa conexiunea VPN trebuie să definiți interfața la care se aplică.

Definirea interfeței pentru regulile de filtru VPN

După ce v-ați configurat regulile pachet VPN și orice alte reguli de care aveți nevoie, pentru a vă activa conexiunea VPN trebuie să definiți interfața la care se aplică.

Pentru a defini o interfață la care să vă aplicați regulile de filtrare VPN, parcurgeți pașii următori:

Notă: Dacă doar ați configurat regulile pachet VPN, interfața Reguli pachet va fi încă deschisă; deplasați-vă la pasul patru.

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Reguli pachet** și selectați **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creați sau să editați filtre și reguli NAT pentru sistemul dumneavoastră.
3. În fereastra Bine ați venit, selectați **Creare fișier regulă pachet nou** și faceți clic pe **OK**.
4. Din editorul Reguli pachet selectați **Inserare** → **Interfață filtru**.
5. În pagina **General**, selectați **Nume linie** și apoi selectați din lista derulantă descrierea liniei la care se aplică regulile pachet VPN.
6. (opțional) Introduceți o descriere.
7. În pagina **Seturi filtre**, apăsați **Adăugare** pentru a adăuga fiecare nume de set pentru filtrele pe care tocmai le-ați configurat.
8. Faceți clic pe **OK**.
9. Salvați fișierul cu regulile dumneavoastră. Fișierul este salvat în sistemul de fișiere integrat de pe sistemul dumneavoastră cu extensia .i3p.

Notă: Nu vă salvați fișierul în următorul director:

/QIBM/UserData/OS400/TCPIP/RULEGEN

Acest director este doar folosit doar de sistem. Dacă aveți nevoie să folosiți comanda RMVTCPTBL *ALL să dezactivați regulile pachet, comanda va șterge toate fișierele din acest director.

După ce definiți o interfață pentru regulile dumneavoastră de filtrare, trebuie să le activați înainte de a putea porni VPN.

Concepte înrudite

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Operații înrudite

“Configurarea unei reguli filtrare politici” la pagina 48

Folosiți aceste informații pentru a afla cum să editați regulile de filtrare politici.

“Activarea regulilor pachet VPN”

Trebuie să activați regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Activarea regulilor pachet VPN

Trebuie să activați regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Nu puteți activa (sau dezactiva) regulile pachet când aveți conexiuni VPN care rulează pe sistemul dumneavoastră. Așa că, înainte să vă activați regulile de filtrare VPN, asigurați-vă că nu există conexiuni active asociate cu ele.

Dacă v-ați creat conexiunile VPN cu vrăjitorul Conexiune nouă, puteți alege să aveți activate regulile asociate, automat, pentru dumneavoastră. Țineți cont că, dacă sunt active alte reguli pachet pe oricare din interfețele pe care le specificați, regulile de filtrare ale politicii VPN le vor înlocui.

Dacă alegeți să vă activați regulile generate VPN folosind Editorul reguli pachet, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Reguli pachete** și selectați **Activare**. Aceasta deschide caseta de dialog **Activare reguli pachet**.
3. Selectați dacă vreți să activați doar regulile generate VPN, doar un fișier selectat sau ambele variante. Puteți alege ultima variantă, de exemplu, dacă aveți diverse reguli PERMIT și DENY pe care doriți să le impuneți pe interfață în plus față de regulile generate VPN.
4. Selectați interfața pe care vreți să activați regulile. Puteți alege să activați pe o anumită interfață, pe un identificator punct-la-punct sau pe toate interfețele și toți identificatorii punct-la-punct.
5. Faceți clic pe **OK** în caseta de dialog pentru a confirma ca vreți să verificați și să activați regulile pe interfața sau interfețele specificate. După ce ați apăsat OK, sistemul verifică regulile de erori sintactice și semantice și raportează rezultatele într-o fereastră mesaj din josul editorului. Pentru mesajele de eroare care sunt asociate cu un fișier anume și un număr de linie, puteți apăsa clic dreapta pe eroare și selecta **Mergi la linie** pentru a evidenția eroarea în fișier.

După ce vă activați regulile de filtrare, vă puteți porni conexiunea VPN.

Concepte înrudite

“Configurarea regulilor de pachete VPN” la pagina 46

Dacă creați o conexiune pentru prima dată, permiteți-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteți face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăți pentru a vă configura conexiunea.

Operații înrudite

“Configurarea conexiunilor sigure VPN” la pagina 44

După ce ați configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configurați conexiunea sigură.

“Definirea interfeței pentru regulile de filtru VPN” la pagina 49

După ce v-ați configurat regulile pachet VPN și orice alte reguli de care aveți nevoie, pentru a vă activa conexiunea VPN trebuie să definiți interfața la care se aplică.

“Pornirea unei conexiuni VPN”

Finalizați această operație pentru a porni conexiuni pe care le inițiați local.

Configurarea TFC (Traffic Flow Confidentiality)

Dacă politica de date este configurată pentru modul Tunel puteți folosi TFC (Traffic Flow Confidentiality) pentru a ascunde lungimea reală a pachetelor de date transferate peste o conexiune VPN.

TFC adăugă blocuri extra pachetelor care sunt trimise și trimite pachete false de diferite lungimi la intervale aleatorii pentru a ascunde lungimea reală a pachetelor. Folosiți TFC pentru o securitate suplimentară împotriva atacatorilor care ar putea ghici tipul de date care se trimit din lungimea pachetului. Când activați TFC câștigați mai multă securitate, dar pierdeți la performanța sistemului. De aceea, trebuie să testați performanța sistemului înainte și după ce activați TFC pe co conexiune VPN. TFC nu este negociat de IKE și utilizatorul va activa TFC numai când ambele sisteme îl suportă.

Pentru a activa TFC pe o conexiune VPN, urmați acești pași:

1. În Navigator iSeries, expandați serverul > **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate** → **Toate conexiunile**.
2. Faceți clic dreapta pe conexiunea pe care vreți să activați TFC și selectați **Proprietăți**.
3. În fișa **General** selectați **Folosire TFC (Traffic Flow Confidentiality) în modul Tunel**.

Configurarea ESN (Extended Sequence Number)

Puteți folosi ESN (Extended Sequence Number) pentru a crește rata de transfer al datelor pentru conexiunea VPN.

Dacă folosiți protocolul AH sau protocolul ESP și AES ca algoritm de criptare puteți dori să activați ESN. ESN vă permite să transmiteți volume mari de date la o viteză mare fără să fie necesară retransmiterea cheilor (re-keying). Conexiunea VPN folosește numere de ordine pe 64 de biți în locul numerelor pe 32 de biți peste IPSec. Folosind numere de ordine de 64 de biți permite mai mult timp înainte de retransmiterea cheilor, care împiedică epuizarea și minimizarea folosirii resurselor de sistem.

Pentru a activa ESN pe o conexiune VPN, urmați acești pași:

1. În Navigator iSeries, expandați serverul > **Rețea** → **Politici IP** → **VPN**
2. Faceți clic dreapta pe **VPN** și selectați **Proprietăți**.
3. În fișa **General** selectați **Folosire ESN (Extended Sequence Number)**.

Pornirea unei conexiuni VPN

Finalizați această operație pentru a porni conexiuni pe care le inițiați local.

Aceste instrucțiuni pleacă de la premisa că ați configurat corespunzător conexiunea VPN. Urmăriți acești pași pentru a porni conexiunea VPN:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Dacă serverul VPN nu este pornit, faceți clic dreapta pe **Rețea privată virtuală** și selectați **Pornire**. Aceasta pornește serverul VPN.
3. Asigurați-vă că regulile dumneavoastră pachet sunt activate.
4. Expandați **VPN** → **Conexiuni securizate**.
5. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
6. Faceți clic dreapta pe conexiunea pe care vreți să o porniți și selectați **Pornire**. Pentru a porni mai multe conexiuni, selectați fiecare conexiune pe care doriți să o porniți, faceți clic dreapta și selectați **Pornire**.

Operații înrudite

“Activarea regulilor pachet VPN” la pagina 50

Trebuie să activați regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Administrarea VPN

Describe diferitele operații cu care puteți să vă gestionați conexiunile VPN active (de exemplu să le modificați, să le monitorizați sau să le ștergeți).

Utilizați interfața VPN din Navigator iSeries pentru a manipula toate task-urile de gestiune, inclusiv:

Setarea atributelor implicite pentru conexiunile dumneavoastră

Valorile implicite apar în panourile pe care le folosiți să creați noi politici și conexiuni. Puteți seta valori implicite pentru nivelurile de securitate, pentru administrarea sesiunilor de chei, pentru duratele de viață ale cheilor și pentru duratele de viață ale conexiunilor.

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

Pentru a seta valorile de securitate implicite pentru conexiunile dumneavoastră VPN, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic pe **Rețea privată virtuală** și selectați **Valori implicite**.
3. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
4. Apăsați **OK** după ce ați completat fiecare din paginile de proprietăți.

Resetarea conexiunilor în starea de eroare

Refacerea conexiunilor dintr-o eroare le întoarce la starea idle.

Pentru a reîmprospăta o conexiune care este în stare de eroare, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea pe care vreți să o resetați și selectați **Resetare**. Aceasta resetează conexiunea la starea inactiv. Pentru a reseta mai multe conexiuni care sunt în stare de eroare, selectați fiecare conexiune pe care doriți să o resetați, faceți clic dreapta și selectați **Resetare**.

Vizualizarea informației de eroare

Finalizați această operație pentru a vă ajuta să determinați de ce conexiunea dumneavoastră are o eroare.

Pentru a vizualiza informațiile despre conexiunile eronate, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea eronată pe care vreți să o vedeți și selectați **Informații despre eroare**.

Operații înrudite

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Vizualizarea atributelor conexiunilor active

Finalizați această operație pentru a verifica starea și alte atribute ale conexiunilor dumneavoastră active.

Pentru a vedea atributele curente ale unei conexiuni active sau la cerere, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea activă sau la cerere pe care doriți să o vizualizați și selectați **Proprietăți**.
4. Mergeți la pagina **Atribute curente** pentru a vedea atributele conexiunii.

De asemenea, puteți vedea atributele tuturor conexiunilor din fereastra Navigator iSeries. În mod implicit, singurele atribute care sunt afișate sunt Stare, Descriere și Tipul conexiunii. Puteți schimba ce date vor fi afișate prin următorii pași:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Din meniul **Obiecte**, selectați **Coloane**. Aceasta deschide o casetă de dialog care vă permite să selectați care atribute vreți să le afișați în fereastra Navigator iSeries.

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

Concepte înrudite

“Mesaje de eroare comune ale managerului de conexiune VPN” la pagina 66

Descrie câteva dintre cele mai obișnuite mesaje de eroare ale managerului de conexiune VPN pe care le puteți întâlni.




Folosirea urmării serverului VPN (VPN server trace)

Vă permite să configurați, să porniți, să opriți și să vizualizați urmările server VPN Connection Manager și VPN Key Manager. Acesta este similar cu folosirea comenzii TRCTCPAPP *VPN din interfața bazată pe caractere cu excepția că puteți vedea urmărirea cât timp o conexiune este activă.

Pentru a vizualiza o urmărire de server VPN, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **VPN**, selectați **Unelte de diagnosticare** și **Urmărire server**.

Pentru a specifica tipul de urmărire pe care doriți să-l genereze VPN Key Manager și VPN Connection Manager, parcurgeți pașii următori:

1. Din fereastra **Rețea privată virtuală**, apăsați  (Opțiuni).
2. În pagina **Manager conexiuni**, specificați ce tip de urmărire doriți să ruleze serverul Connection Manager.
3. În pagina **Manager chei**, specificați ce tip de urmărire doriți să ruleze serverul Key Manager.
4. Apăsați **Ajutor** dacă aveți întrebări despre cum să completați o pagină sau oricare din câmpurile ei.
5. Apăsați **OK** pentru a salva modificările.
6. Apăsați  (Pornire) pentru a porni urmărirea. Apăsați  (Reîmprospătare) periodic pentru a vedea ultimele informații de urmărire.

Vizualizarea fișierelor jurnal job ale serverului VPN

Urmați aceste instrucțiuni pentru a vedea fișierele jurnal de joburi din VPN Key Manager și VPN Connection Manager.

Pentru a vedea fișierele jurnal job curente ale VPN Key Manager sau ale VPN Connection Manager, urmați pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Rețea privată virtuală**, selectați **Unelte de diagnoză** și apoi selectați istoricul jobului de server pe care doriți să-l vizualizați.

Vizualizarea atributelor Asocierilor de securitate (Security Associations - SA)

Finalizați această operație pentru a afișa atributele Asocierilor de securitate (Security Associations - SAs) care sunt asociate cu o conexiune activată.

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

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea activă corespunzătoare și selectați **Asocieri de securitate**. Fereastra rezultată vă permite să vizualizați proprietățile fiecărei dintre SA-urile asociate cu o conexiune specifică.

Oprirea unei conexiuni VPN

Finalizați această operație pentru a opri conexiuni active.

Pentru a opri o conexiune activă sau la-cerere, parcurgeți pașii următori:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea pe care vreți să o opriți și selectați **Oprire**. Pentru a opri mai multe conexiuni, selectați fiecare conexiune pe care doriți să o opriți, faceți clic dreapta și selectați **Oprire**.

Ștergerea obiectelor de configurare VPN

Înainte să ștergeți un obiect de configurare VPN din baza de date de politici VPN, asigurați-vă că înțelegeți cum afectează alte conexiuni și grupuri de conexiuni VPN.

Dacă sunteți sigur că aveți nevoie să ștergeți o conexiune VPN din baza de date de politici VPN, executați următorii pași:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Apăsați **Toate conexiunile** pentru a afișa o listă a conexiunilor în panoul din dreapta.
3. Faceți clic dreapta pe conexiunea pe care vreți să o ștergeți și selectați **Ștergere**.

Depanarea VPN

Consultați acest subiect când aveți probleme cu conexiunile VPN.

VPN este o tehnologie complexă care se schimbă rapid și care necesită cel puțin cunoștințe de bază privind tehnologiile IPSec obișnuite. Trebuie de asemenea să fiți familiarizat cu regulile pachet IP deoarece VPN necesită câteva reguli filtru pentru a funcționa corect. Din cauza acestei complexități, s-ar putea să experimentați, din când în când, probleme cu conexiunile dumneavoastră VPN. Depanarea VPN nu este întotdeauna o sarcină ușoară. Trebuie să vă înțelegeți mediile de rețea și de sistem, cât și componentele pe care le folosiți când obișnuiți să le gestionați. Următoarele subiecte vă sugerează indicii despre cum să depanați problemele diverse pe care le puteți întâlni când folosiți VPN:

Inițierea în depanarea VPN

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Există câteva moduri de a începe analizarea problemelor VPN:

1. Asigurați-vă întotdeauna că ați aplicat cele mai recente corecții temporare de program (PTF-uri)?
2. Asigurați-vă că îndepliniți Cerințele minime pentru setarea VPN.
3. Revedeți orice mesaj de eroare găsit în fereastra Informații de eroare sau în istoricele de job ale serverului VPN, atât pentru sistemul local, cât și pentru cel la distanță. De fapt când depanați probleme de conexiuni VPN, este adesea necesar să priviți ambele capete ale conexiunii. Mai departe, trebuie să luați în considerare faptul că trebuie

să verificați patru adrese: capetele local și la distanță ale conexiunii, care sunt adresele unde IPSec este aplicat la pachete, și punctele finale de date local și la distanță, care sunt adrese sursă și destinație ale pachetelor IP.

4. Dacă mesajele de eroare găsite nu aduc suficiente informații pentru a rezolva problema, verificați jurnalul filtrului IP.
5. Urmărirea comunicației pe sistem vă oferă un alt loc în care găsiți informații generale despre faptul că sistemul local primește sau trimite cereri de conexiune.
6. Comanda Trace TCP Application (TRCTCPAPP) furnizează o altă cale de a izola probleme. Tipic, IBM Service utilizează TRCTCPAPP pentru a obține o ieșire de urmărire pentru a analiza problemele de conexiune.

Concepte înrudite

“Cerințele pentru setarea VPN” la pagina 35

Folosiți aceste informații pentru a vă asigura că îndepliniți cerințele minime pentru crearea unei conexiuni VPN.

“Depanarea VPN cu istoricul de job VPN” la pagina 65

Describe diversele istorice de job pe care le folosește VPN.

“Depanarea VPN cu urmărirea comunicațiilor” la pagina 71

Operații înrudite

“Vizualizarea informației de eroare” la pagina 52

Finalizați această operație pentru a vă ajuta să determinați de ce conexiunea dumneavoastră are o eroare.

“Depanarea VPN cu jurnalul QIPFILTER” la pagina 61

Vedeți aceste informații pentru a afla despre regulile de filtrare VPN.

“Pornirea unei conexiuni VPN” la pagina 51

Finalizați această operație pentru a porni conexiuni pe care le inițiați local.

Alte lucruri de verificat

Dacă apare o eroare după ce setați o conexiune și nu sunteți sigur unde a apărut eroarea în rețea, încercați să reduceți complexitatea mediului dumneavoastră de lucru. De exemplu, în loc să investigați toate părțile unei conexiuni VPN o dată, începeți cu conexiunea IP. Lista următoare vă dă câteva indicații de bază despre cum să porniți analizarea problemelor VPN, de la cele mai simple conexiuni IP la mai complexe conexiuni VPN:

1. Începeți cu o configurație IP între gazda locală și cea de la distanță. Înlăturați orice filtre IP din interfața folosită de sistemul local și cel la distanță pentru comunicație. Puteți face ping de la gazda locală la gazda de la distanță?

Notă: Amintiți-vă să dați prompt pe comanda PING; introduceți adresa sistemului la distanță și folosiți PPF10 pentru parametri suplimentari, apoi introduceți adresa IP locală. Aceasta este important mai ales când aveți mai multe interfețe fizice și logice. Asigurați-vă că sunt plasate adresele corecte în pachetele PING.

Dacă răspundeți **da**, treceți la pasul 2. Dacă răspundeți **nu**, verificați configurația IP, starea interfeței și intrările de rutare. Dacă configurarea este corectă, folosiți monitorizarea comunicației pentru a verifica de exemplu că cererea IP părăsește sistemul. Dacă trimiteți o cerere PING și nu primiți răspuns, problema este probabil în rețea sau la sistemul la distanță.

Notă: Pot exista rutere sau firewall-uri intermediare care filtrează pachetele IP și ar putea opri pachetele PING. PING este bazat de obicei pe protocolul ICMP. Dacă PING reușește, știți că există legătura. Dacă PING nu reușește, știți doar că a eșuat PING. Ați putea încerca alte protocoale IP între cele două sisteme, de exemplu Telnet sau FTP, pentru a testa conexiunea.

2. Verificați regulile de filtrare pentru VPN și asigurați-vă că sunt activate. Pornește filtrarea cu bine? Dacă răspundeți **da**, treceți la pasul 3. Dacă răspundeți **nu**, verificați mesajele de eroare din fereastra Reguli pachet din Navigator iSeries. Asigurați-vă că regulile de filtrare nu specifică Traducerea Adreselor de Rețea (NAT) pentru traficul VPN.
3. Porniți conexiunea dumneavoastră VPN. Pornește conexiunea cu bine? Dacă răspundeți **da**, mergeți la pasul 4. Dacă răspundeți **nu**, verificați istoricele de job QTOVMAN și QTOKVPNIKE pentru erori. Când folosiți VPN-ul, furnizorul dumneavoastră de servicii Internet (ISP) și fiecare gateway de securitate din rețeaua dumneavoastră trebuie să suporte protocoalele Authentication Header (AH) și Encapsulated Security Payload (ESP). Dacă alegeți să folosiți AH sau ESP depinde de propunerile pe care le definiți pentru conexiunile dumneavoastră VPN.

4. Puteți activa o sesiune utilizator peste conexiunea VPN? Dacă răspundeți **da**, atunci conexiunea VPN funcționează așa cum ați cerut. Dacă răspundeți **nu**, atunci verificați regulile pachet și grupurile cheie dinamică VPN și conexiunile pentru definițiile filtru care nu permit traficul utilizator pe care îl vreți.

Erorile obișnuite de configurare VPN și cum se pot repara

Aceste informații identifică cele mai comune erori ale utilizatorilor și furnizează soluții posibile.

Această secțiune descrie câteva dintre cele mai obișnuite probleme care apar cu VPN și vă face legătura cu sugestii și cum să le rezolvați.

Notă: Când configurați VPN, creați 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 și Conexiuni sigure. Astfel, când aceste informații se referă la un obiect, se referă la una sau mai multe dintre aceste părți ale VPN.

Mesaj de eroare VPN: TCP5B28

Când încercați să activați reguli de filtrare pe o interfață, ajungeți la acest mesaj: TCP5B28 CONNECTION_DEFINITION order violation

Simptom:

Când încercați să activați reguli de filtrare pe o anumită interfață, primiți acest mesaj de eroare:
TCP5B28: Violare ordine CONNECTION_DEFINITION

Soluția posibilă:

Regulile filtru pe care încercați să le activați conțineau definiții de conexiune care au fost ordonate diferit decât în setul de reguli activat anterior. Cel mai ușor mod de a rezolva această eroare este de a activa fișierul cu reguli pe **toate interfețele** în loc de o anumită interfață.

Mesaj de eroare VPN : Articolul nu a fost găsit

Când faceți clic dreapta pe un obiect VPN și selectați fie **Proprietăți** sau **Ștergere**, ajungeți la mesajul care spune **Articol negăsit**.

Simptom:

Când faceți clic dreapta pe un obiect din fereastra VPN și selectați **Proprietăți** sau **Ștergere**, apare mesajul următor:



Soluția posibilă:

- Poate ați șters sau redenumit obiectul și nu ați reîmprospătat încă fereastra. Ca urmare, obiectul apare încă în fereastra Rețea privată virtuală. Pentru a verifica dacă este așa, din meniul **Vizualizare**, selectați **Reîmprospătare**. Dacă obiectul apare tot în fereastra Rețea privată virtuală, continuați cu articolul următor din această listă.
- Când ați configurat proprietățile pentru obiect, s-ar putea să fi survenit o eroare de comunicație între serverul VPN și sistemul dumneavoastră. Multe dintre obiectele care apar în fereastra VPN au legătură cu mai mult de un obiect din baza de date de politici VPN. Aceasta înseamnă că erorile de comunicație pot face ca unele obiecte din baza de date să fie legate de un obiect din VPN. De fiecare dată când creați sau actualizați un obiect, va apărea o eroare la pierderea sincronizării. Singurul mod de a rezolva problema este să selectați **OK** în fereastra de eroare. Aceasta lansează tabelul de proprietăți al obiectului cu eroare. Doar

câmpul de nume are o valoare în el. Toate celelalte sunt goale (sau conțin valori implicite). Introduceți atributele corecte ale obiectului și selectați **OK** pentru a salva schimbările.

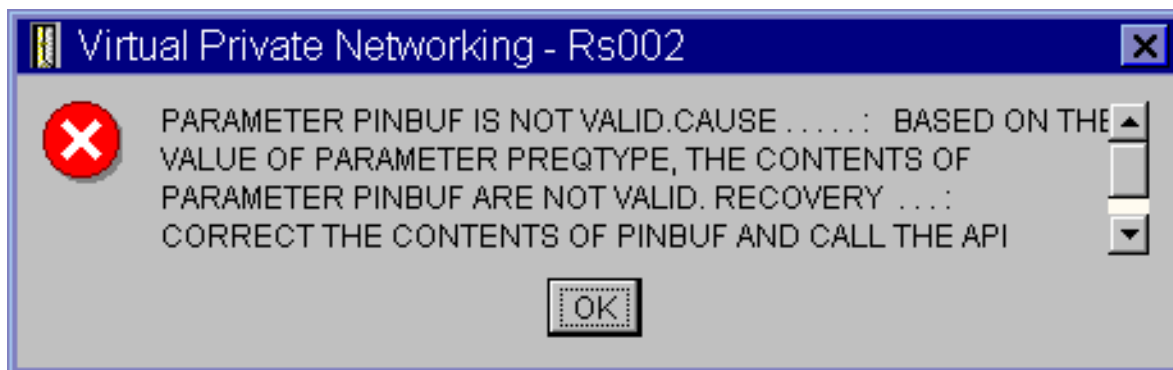
- O eroare similară apare când încercați să ștergeți obiectul. Pentru a rezolva această problemă, completați tabelul de proprietăți gol care se deschide când faceți clic pe **OK** în mesajul de eroare. Acesta actualizează orice legături la baza de date VPN care erau pierdute. Acum puteți șterge obiectul.

Mesaj de eroare VPN: Parametrul PINBUF nu este valid

Când încercați să realizați o conexiune, ajungeți la mesajul care spune: **PARAMETER PINBUF IS NOT VALID...**

Simptom:

Când încercați să porniți o conexiune, apare un mesaj ca următorul:



Soluția 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, asigurați-vă că toate obiectele folosesc numai litere mari sau schimbați localizarea sistemului.

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

Când selectați **Proprietăți** pentru o conexiune de chei dinamice, ajungeți la o eroare care spune că serverul nu poate găsi serverul de chei la distanță specificat de dumneavoastră.

Simptom:

Când selectați **Proprietăți** pentru o conexiune de chei dinamice, apare un mesaj ca următorul:



Soluția posibilă:

Aceasta se întâmplă când creați o conexiune cu un anumit identificator de server de chei la distanță și apoi serverul de chei de la distanță este șters din grupul său de chei dinamice. Pentru a rezolva această eroare, apăsați **OK** pe mesajul de eroare. Aceasta deschide foaia cu proprietăți pentru conexiunea de chei dinamice care are eroarea. De aici, puteți să adăugați serverul de chei la distanță înapoi în grupul de chei dinamice sau selectați alt identificator server de chei la distanță. Apăsați **OK** pe foaia de proprietăți pentru a vă salva modificările.

Mesaj de eroare VPN: Nu se poate actualiza obiectul

Când selectați **OK** pe foaia de proprietăți pentru un grup de chei dinamice sau o conexiune manuală, ajungeți la mesajul care vă spune că sistemul dumneavoastră nu poate actualiza obiectul.

Simptom:

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



Soluția posibilă:

Această eroare apare când o conexiune activă folosește obiectul pe care încercați să-l modificați. Nu puteți modifica un obiect dintr-o conexiune activă. Pentru a modifica un obiect, identificați conexiunea activă corespunzătoare, apoi faceți clic dreapta pe ea și selectați **Oprire** din meniul contextual.

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

Ajungeți la mesajul care spune că sistemul nu poate cripta cheile dumneavoastră pentru că valoarea QRETSVRSEC trebuie să fie pusă pe 1.

Simptom:

Apare următorul mesaj de eroare:



Soluția 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 și cheile pentru algoritmi dintr-o conexiune manuală nu pot fi memorate în baza de date a politicii VPN. Pentru a rezolva această problemă, folosiți o sesiune de emulare 5250 către sistemul dumneavoastră. Tastați `wrksysval` în linia de comandă și apăsați **Enter**. Căutați QRETSVRSEC în listă și tastați 2 (modificare) lângă el. În panoul alăturat, tastați 1 și apăsați **Enter**.

Concepte înrudite

“Eroare VPN: Toate cheile sunt goale” la pagina 59

Când vizualizați proprietățile unei conexiuni manuale, toate cheile prepartajate și cheile algoritmului pentru conexiune sunt goale.

Mesaj de eroare VPN: CPF9821

Când încercați să expandați sau să deschideți containerul Politici IP din Navigator iSeries, apare mesajul CPF9821-Fără autorizare pentru programul QTFRPRS din biblioteca QSYS.

Simptom:

Când încercați să expandați containerul Politici IP din Navigator iSeries, apare mesajul CPF9821 - Fără autorizare pentru programul QTFRPRS din biblioteca QSYS.

Soluția posibilă:

Puteți să nu aveți autorizarea necesară pentru a extrage starea curentă a regulilor de pachete sau managerului de conexiune VPN. Asigurați-vă că aveți autoritatea *IOSYSCFG pentru a căpăta acces la funcțiile regulă pachet din Navigatorul iSeries.

Eroare VPN: Toate cheile sunt goale

Când vizualizați proprietățile unei conexiuni manuale, toate cheile prepartajate și cheile algoritmului pentru conexiune sunt goale.

Simptom:

Toate cheile prepartajate și cheile pentru algoritmi de conexiune manuală sunt goale.

Soluția posibilă:

Aceasta se întâmplă când valoarea de sistem QRETSVRSEC este setată înapoi la 0. Setarea acestei valori de sistem la 0 șterge toate cheile din baza de date a politicii VPN. Pentru a rezolva această problemă trebuie să setați valoarea de sistem la 1 și apoi să reintroduceți toate cheile. Consultați Mesaj de eroare: Nu se pot cripta cheile pentru informații suplimentare despre cum se realizează aceasta.

Concepte înrudite

“Mesaj de eroare VPN: Nu se poate cripta cheia...” la pagina 58

Ajungeți la mesajul care spune că sistemul nu poate cripta cheile dumneavoastră pentru că valoarea QRETSVRSEC trebuie să fie pusă pe 1.

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

Prima dată când folosiți interfața de reguli pachete în iSeries, un ecran de deschidere de sesiune apare pentru un sistem diferit de cel curent.

Simptom:

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

Soluția posibilă:

Reguli pachet folosește unicode pentru a memora regulile de securitate pachet în sistemul de fișiere integrat. Înregistrarea suplimentară permite iSeries Access pentru Windows să obțină tabela de conversie corespunzătoare pentru unicode. Aceasta se va întâmpla doar o dată.

Eroare VPN: Starea conexiunii este goală în fereastra Navigator iSeries

O conexiune nu are nici o valoare în coloana **Stare** din fereastra Navigator iSeries.

Simptom:

O conexiune nu are nici o valoare în coloana **Stare** din fereastra Navigator iSeries.

Soluția posibilă:

Valoarea goală de stare arată că conexiunea este în curs de pornire. Adică nu este încă pornită, dar nu a întors încă o eroare. Atunci când reîmprospătați fereastra, conexiunea va afișa o stare de Eroare, Activă, La-cerere sau Inactivă.

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

După ce opriți o conexiune, fereastra Navigator iSeries arată conexiunea încă activă.

Simptom:

După ce opriți o conexiune, fereastra Navigator iSeries arată conexiunea încă activă.

Soluția posibilă:

Aceasta se întâmplă de obicei pentru că nu ați reîmprospătat fereastra Navigator iSeries. Astfel, fereastra conține informații vechi. Pentru a repara aceasta, de la meniul **Vizualizare**, selectați **Reîmprospătare**.

Eroare VPN : 3DES nu este o soluție pentru criptare

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

Simptom:

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

Soluția posibilă:

Cel mai probabil, aveți 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 restricțiilor la lungimile de cheie.

Eroare VPN: Afișare neașteptată de coloane în fereastra Navigator iSeries

Setați coloanele pe care vreți să le afișați în fereastra Navigator iSeries pentru conexiunile dumneavoastră VPN; apoi, când vă uitați la ele mai târziu, vor fi afișate alte coloane.

Simptom:

Setați coloanele pe care vreți să le afișați în fereastra Navigator iSeries pentru conexiunile dumneavoastră VPN; apoi, când vă uitați la ele mai târziu, vor fi afișate coloane diferite.

Soluția posibilă:

Când schimbați 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 dezactivate

Când încercați să dezactivați setul curent de reguli de filtrare, apare mesajul, Regulile active nu pot fi dezactivate în fereastra de rezultate.

Simptom:

Când încercați să dezactivați setul curent de reguli de filtrare, apare mesajul, Regulile active nu pot fi dezactivate în fereastra de rezultate.

Soluția posibilă:

De obicei, acest mesaj arată că există cel puțin o conexiune VPN activă. Trebuie să opriți fiecare conexiune care starea **activ**. Pentru aceasta, faceți clic dreapta pe fiecare conexiune activă și selectați **Oprire**. Puteți dezactiva acum regulile filtru.

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

Când creați o conexiune cu cheie dinamică, specificați un grup de chei dinamice și un identificator pentru serverul de chei la distanță. Mai târziu, când vedeți proprietățile obiectului conexiunii înrudite, pagina General a foii de proprietăți afișează același identificator de server de chei la distanță, dar un grup de chei dinamice diferit.

Simptom:

Când creați o conexiune cu cheie dinamică, specificați un grup de chei dinamice și un identificator pentru serverul de chei la distanță. Mai târziu, când selectați **Proprietăți** pentru obiectul conexiune înrudit, pagina **General** a tabelului de proprietăți afișează același identificator al serverului de chei la distanță, dar un alt grup de chei dinamice.

Soluția posibilă:

Identificatorul este singura informație memorată în baza de date a politicii VPN care se referă la serverul de chei la distanță al conexiunii de chei dinamice. Când VPN verifică o politică pentru un server de chei la distanță, caută primul grup de chei dinamice care are în el identificatorul serverului de chei dinamice la distanță. Deci când vedeți proprietățile pentru una dintre aceste conexiuni, ea folosește același grup de chei dinamice găsit de VPN. Dacă nu doriți să asociați grupul de chei dinamice cu acel server de chei dinamice, puteți realiza una dintre următoarele acțiuni:

1. Înlăturați serverul de chei la distanță din grupul de chei dinamice.

2. Expandați **După grupuri** în panoul din stânga al interfeței VPN și selectați și trageți grupul cheie dinamic pe care îl vreți în vârful tabelii din panoul din dreapta. Aceasta asigură că VPN verifică întâi acest grup de chei dinamice pentru serverul de chei la distanță.

Depanarea VPN cu jurnalul QIPFILTER

Vedeți aceste informații pentru a afla despre regulile de filtrare VPN.

Jurnalul QIPFILTER se află în biblioteca QUSRSYS și conține informații despre seturi de reguli de filtrare, cât și informații despre faptul dacă o datagramă IP a fost permisă sau respinsă. Înregistrarea în istoric se realizează pe baza opțiunii de jurnalizare pe care o specificați în regulile dumneavoastră de filtrare.

Operații înrudite

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Cum să activați jurnalul Filtru pachet IP?

Utilizați editorul Reguli pachet din Navigator iSeries pentru a activa jurnalul QIPFILTER. Trebuie să activați funcția de înregistrare în istoric pentru fiecare regulă filtru în parte. Nu există nici o funcție care permite înregistrarea în istoric pentru toate datagramele IP care intră sau ies din sistem.

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

Următorii pași descriu cum să activați jurnalizarea pentru o anumită regulă de filtrare:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP**.
2. Faceți clic dreapta pe **Reguli pachet** și selectați **Configurare**. Aceasta afișează interfața Reguli pachet.
3. Deschideți un fișier cu reguli de filtrare existent.
4. Faceți dublu clic pe regula de filtrare pe care doriți s-o jurnalizați.
5. Pe pagina **General**, selectați **FULL** în câmpul **Jurnalizare** ca în caseta de dialog de mai sus. Aceasta activează înregistrarea în istoric pentru această regulă de filtrare.
6. Faceți clic pe **OK**.
7. Salvați și activați fișierul modificat cu regula de filtrare.

Dacă o datagramă IP se potrivește cu definițiile regulii de filtrare, este făcută o intrare în jurnalul QIPFILTER.

Cum să folosiți jurnalul QIPFILTER?

i5/OS creează automat jurnalul prima oară când activați filtrarea pachet IP. Pentru a vedea detaliile specifice-intrării din jurnal, puteți afișa intrările din jurnal pe ecran sau puteți folosi un fișier de ieșire.

Copiind intrările din jurnal în fișierul de ieșire, puteți vedea cu ușurință intrările folosind utilitare de interogare așa cum este Query/400 sau SQL. Puteți de asemenea să vă scrieți propriile programe HLL pentru a procesa intrările din fișierele de ieșire.

Următorul este un exemplu de comandă Afișare jurnal (DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTYP((TF)) OUTPUT(*OUTFILE)
      OUTFILFMT(*TYPE4) OUTFILE(biblioteca/fișier) ENTDTALEN(*VARLEN *CALC)
```

Folosiți următorii pași pentru a copia intrările din jurnalul QIPFILTER în fișierul de ieșire:

1. Creați o copie a fișierului de ieșire 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(biblioteca)
NEWOBJ(fișier)

2. Folosiți comanda Afișare jurnal (DSPJRN) pentru a copia intrările din jurnalul QUSRSYS/QIPFILTER în fișierul de ieșire pe care l-ați creat în pasul anterior.

Dacă copiați DSPJRN într-un fișier de ieșire care nu există, sistemul creează un fișier pentru dumneavoastră, dar acesta nu conține descrierile câmpului corecte.

Notă: Jurnalul QIPFILTER conține doar intrări de permitere sau respingere pentru regulile filtru unde opțiunea de jurnalizare este setată pe FULL. De exemplu, dacă setați doar reguli filtru PERMIT, datagramele IP care nu sunt permise explicit sunt refuzate. Pentru aceste datagrame respinse, nici o intrare nu este adăugată la jurnal. Pentru analiza problemei puteți să adăugați o regulă filtru care respinge în mod explicit orice alt trafic și realizează jurnalizare FULL. Apoi, veți obține intrările DENY din jurnal pentru toate datagramele IP care sunt respinse. Din motive de performanță, nu este recomandat să activați jurnalizarea pentru toate regulile filtru. O dată ce seturile dumneavoastră de filtrare sunt testate, reduceți jurnalizarea la un subset de intrări folositor.

Vedeți Câmpuri din jurnalul QIPFILTER pentru o tabelă care descrie fișierul de ieșire QIPFILTER.

Câmpurile din jurnalul QIPFILTER

Următoarea tabelă descrie câmpurile din fișierul de ieșire 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 | Amprentă 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*, spațiu 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 acțiune filtru |
| TFPDIR | 1 | N | Direcție pachet IP | O este ieșire, I este intrare |
| TFRNUM | 5 | N | Număr regulă | Se aplică la numărul regulii din fișierul activ de reguli |
| TFACT | 6 | N | Acțiunea filtru efectuată | PERMIT, DENY sau IPSEC |

| Nume câmp | Lungime câmp | Numeric | Descriere | Comentarii |
|-----------|--------------|---------|----------------------|---|
| 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 | Gunoii dacă TFPROT= 1 (ICMP) |
| TFDSTA | 15 | N | Adresa IP destinație | |
| TFDSTP | 5 | N | Port destinație | Gunoii dacă TFPROT= 1 (ICMP) |
| TFTEXT | 76 | N | Text suplimentar | Conține descriere dacă TFREVT= L* sau U* |

Depanarea VPN cu jurnalul QVPN

Furnizează informații despre traficul IP și despre conexiuni.

VPN folosește un jurnal separat pentru a înregistra informațiile despre trafic IP și conexiuni numit jurnal QVPN. QVPN este memorat în biblioteca QUSRSYS. Codul jurnalului este M și tipul jurnalului este TS. Veți folosi rar intrările din jurnal zilnic. În schimb, s-ar putea să le găsiți utile pentru depanarea și verificarea că sistemul, cheile și conexiunile dumneavoastră funcționează în modul pe care l-ați specificat. De exemplu, intrările jurnalului vă ajută să înțelegeți ce se întâmplă cu pachetele dumneavoastră de date. De asemenea vă țin la curent cu starea curentă VPN.

Cum să activați jurnalul VPN?

Utilizați interfața rețea privată virtuală din Navigator iSeries pentru a activa jurnalul VPN. Nu există nici o funcție care permite înregistrarea în jurnal pentru toate conexiunile VPN. De aceea, trebuie să activați funcția de înregistrare în istoric pentru fiecare grup cheie dinamic sau conexiune manuală.

Următorii pași descriu cum să activați funcția de jurnalizare pentru un anumit grup de chei dinamice sau conexiune manuală:

1. În Navigator iSeries, expandați **serverul** → **Rețea** → **Politici IP** → **VPN** → **Conexiuni securizate**.
2. Pentru grupuri de chei dinamice, expandați **După grup** și apoi faceți clic dreapta pe grupul de chei dinamice pentru care doriți să activați jurnalizarea și selectați **Proprietăți**.
3. Pentru conexiuni manuale, expandați **Toate conexiunile** și apoi faceți clic dreapta pe conexiunea manuală pentru care doriți să activați jurnalizarea.
4. În pagina **General**, selectați nivelul de jurnalizare pe care îl cereți. Aveți de ales dintre patru opțiuni. Acestea sunt:

Fără Nu apare nici o jurnalizare pentru acest grup de conexiuni.

Toate Jurnalizarea se realizează pentru toate activitățile conexiunii, cum ar fi pornirea sau oprirea unei conexiuni sau reîmprospătarea unei chei, cât și pentru informațiile 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 informații despre traficul IP în jurnalul QIPFILTER, care se află în biblioteca QUSRSYS.

5. Faceți clic pe **OK**.
6. Porniți conexiunea pentru a activa jurnalizarea.

Notă: Înainte de a putea opri jurnalizarea, asigurați-vă de inactivitatea conexiunii. Pentru a schimba starea jurnalizării unui grup de conexiuni, asigurați-vă că nu sunt conexiuni active asociate cu acel grup.

Cum să folosiți jurnalul VPN?

Pentru a vedea detaliile specifice-intrării din jurnalul VPN, puteți afișa intrările din jurnal pe ecran sau puteți folosi un fișier de ieșire.

Copiind intrările din jurnal în fișierul de ieșire, puteți vedea cu ușurință intrările folosind utilitare de interogare așa cum este Query/400 sau SQL. Puteți de asemenea să vă scrieți propriile programe HLL pentru a procesa intrările din fișierele de ieșire. Următorul este un exemplu de comandă Afișare jurnal (DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
      OUTFILE(biblioteca/fișier) ENTDTALEN(*VARLEN *CALC)
```

Folosiți următorii pași pentru a copia intrările din jurnalul VPN în fișierul de ieșire:

1. Creați o copie a fișierului de ieșire furnizat de sistem QSYS/QATOVSOFF într-o bibliotecă utilizator. Puteți face aceasta folosind comanda Creare Obiect Duplicat (CRTDUPOBJ). Următorul este un exemplu de comandă CRTDUPOBJ:

```
CRTDUPOBJ OBJ(QATOVSOFF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(biblioteca)
      NEWOBJ(fișier)
```

2. Folosiți comanda Afișare Jurnal (DSPJRN) pentru a copia intrările din jurnalul QUSRSYS/QVPN în fișierul de ieșire pe care l-ați creat în pasul anterior. Dacă încercați să copiați DSPJRN într-un fișier de ieșire care nu există, sistemul creează un fișier pentru dumneavoastră, dar acesta nu conține descrierile câmpului corecte.

Vedeți Câmpuri jurnal QVPN pentru o tabelă care descrie câmpurile din fișierul de ieșire QVPN.

Câmpurile din jurnalul QVPN

Următoarea tabelă descrie câmpurile din fișierul de ieșire 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 | Intrarea amprentă de timp 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 | |
| TSRESA | 50 | N | Nefolosit | |
| TSESDL | 4 | Y | Lungimea datelor specifice | |

| Nume câmp | Lungime câmp | Numeric | Descriere | Comentarii |
|-----------|--------------|---------|------------------------------------|------------|
| 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 sfârșit | |
| TSCOET | 6 | N | Timpul de sfârșit | |
| TSTRPR | 10 | N | Protocol transport | |
| TSLCAD | 43 | N | Adresa locală a clientului | |
| TSLCPR | 11 | N | Porturi locale | |
| TSRCAD | 43 | N | Adresa de la distanță a clientului | |
| TSCPR | 11 | N | Porturi de la distanță | |
| TSLEP | 43 | N | Punct final local | |
| TSREP | 43 | N | Punct final la distanță | |
| TSCORF | 6 | N | Număr de reîmprospătări | |
| TSRFDA | 8 | N | Data următoarei reîmprospătări | |
| TSRFTI | 6 | N | Timpul următoarei reîmprospătări | |
| TSRFLS | 8 | N | Durata de viață 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 istoricul de job VPN

Descrie diversele istorice de job pe care le folosește VPN.

Când aveți probleme la conexiunile dumneavoastră VPN, este întotdeauna recomandabil să istoricele de job. De fapt există câteva istorice de job care conțin mesaje de eroare și alte informații legate de un mediu VPN.

Este important să analizați istoricele de joburi din ambele părți ale conexiunii dacă ambele sunt sisteme iSeries. Când o conexiune dinamică nu poate porni, este folositor să înțelegeți ce se întâmplă pe serverul de la distanță.

Joburile VPN, QTOVMAN și QTOKVPNIKE, rulează în subsistemul QSYSWRK. Puteți să vizualizați istoricele de job corespunzătoare din Navigator iSeries.

Această secțiune prezintă cele mai importante sarcini pentru un mediu VPN. Lista următoare arată numele jobului și o scurtă explicație a utilității jobului:

QTCPIP

Acest job este jobul de bază care pornește toate interfețele TCP/IP. Dacă aveți probleme fundamentale cu TCP/IP în general, analizați istoricul jobului 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. Istoricul de job asociat conține mesaje pentru fiecare încercare de conectare care eșuează.

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 manager pentru L2TP (Layer Two Tunneling Protocol). Dacă aveți probleme la configurarea unui tunel L2TP, vedeți mesajele din acest istoric de job.

Operații înrudite

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Mesaje de eroare comune ale managerului de conexiune VPN

Descrie câteva dintre cele mai obișnuite mesaje de eroare ale managerului de conexiune VPN pe care le puteți întâlni.

În general, managerul de conexiune VPN reține două mesaje în istoricul de job QTOVMAN când o eroare apare cu o conexiune VPN. Primul mesaj furnizează detalii cu privire la eroare. Puteți vedea informații despre aceste erori în Navigator iSeries făcând clic dreapta pe conexiunea cu eroare și selectând **Informații eroare**.

Al doilea mesaj descrie acțiunea pe care ați încercat-o pentru această conexiune când a apărut eroarea. De exemplu, pornirea sau oprirea ei. Mesajele TCP8601, TCP8602 și 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 [<i>nume conexiune</i>] | Nu s-a putut porni această conexiune VPN datorită unui sau mai multe coduri motiv: <i>0</i> - Un mesaj anterior din istoricul de joburi cu același nume de conexiune VPN are mai multe informații detaliate. <i>1</i> - Configurarea politicii VPN. <i>2</i> - Eșuarea rețelei de comunicații. <i>3</i> - Managerul de chei VPN a eșuat în a negocia o nouă asociere de securitate. <i>4</i> - Punctul final la distanță pentru această conexiune nu este configurat corespunzător. <i>5</i> - Managerul de chei VPN a eșuat să răspundă managerului de conexiune VPN. <i>6</i> - Eșuare de încărcare a conexiunii VPN a componentei de securitate IP. <i>7</i> - Eșuare componentă PPP. | <ol style="list-style-type: none">1. Verificați istoricul de joburi pentru mesaje adiționale.2. Corectați erorile și încercați cererea din nou.3. Folosiți Navigator iSeries pentru a vizualiza starea conexiunii. Conexiunile care nu au putut fi pornite for fi în stare de eroare. |

Mesajele de eroare ale managerului de conexiune VPN

Mesaj

TCP8602 Eroarea a apărut la oprirea conexiunii VPN [*nume conexiune*]

Cauză

Conexiunea VPN specificată s-a cerut să fie oprită, dar nu s-a oprit sau s-a oprit în eroare datorită codului motiv: 0 - Un mesaj anterior din istoricul de joburi cu același nume de conexiune VPN are mai multe informații detaliate. 1 - Conexiunea VPN nu există. 2 - Eșuare de comunicații internă cu managerul de chei VPN. 3 - Eșuare de comunicații internă cu componenta IPsec. 4 - Eșuare de comunicații cu punctul final la distanță de conexiune VPN.

Recuperare

1. Verificați istoricul de joburi pentru mesaje adiționale.
2. Corectări erorile și încercați cererea din nou.
3. Folosiți Navigator iSeries pentru a vizualiza starea conexiunii. Conexiunile care nu au putut fi pornite for fi în stare de eroare.

TCP8604 Pornirea conexiunii VPN [*nume conexiune*] a eșuat

O pornire a acestei conexiuni VPN a eșuat datorită unuia din următoarele coduri eroare: 1 - Nu s-a putut translata numele de gazdă la distanță într-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 inițială pentru conexiunea VPN nu permite specificarea acțiunii. 6 - Un rol sistem pentru conexiunea VPN este inconsistent în informații de la grupul de conexiune. 7 - Rezervat. 8 - Punctele finale de date (servicii și adrese la distanță și locale) a acestei conexiuni VPN sunt inconsistente în informații de la grupul de conexiune. 9 - Tipul identificator nu este valid.

1. Verificați istoricul de joburi pentru mesaje adiționale.
2. Corectări erorile și încercați cererea din nou.
3. Folosiți Navigator iSeries pentru a verifica sau corecta configurația de politică VPN. Asigurați-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.

TCP8605 Managerul de conexiune VPN nu a putut comunica 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. Verificați istoricul de joburi pentru mesaje adiționale.
2. Verificați dacă interfața *LOOPBACK este activă folosind comanda NETSTAT OPTION(*IFC).
3. Terminați serverul VPN folosind comanda ENDTCPSVR SERVER(*VPN). Apoi reporniți serverul VPN folosind comanda STRTCPSRV SERVER(*VPN).
Notă: Aceasta provoacă toate conexiunile VPN să se termine.

Mesajele de eroare ale managerului de conexiune VPN

Mesaj

TCP8606 Managerul de chei VPN nu a putut stabili asocierea de securitate cerută pentru conexiunea [*nume conexiune*]

Cauză

Managerul de chei VPN nu a putut stabili asocierea de securitate cerută datorită unuia din următoarele coduri eroare: *24* - A eșuat autentificarea de către managerul de chei VPN a cheii conexiunii. *8300* - Eșuarea 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 distanță. *8308* - Nu s-a găsit nici o cheie prepartajată la distanță. *8327* - E expirat timpul negocierilor de chei de conexiune a managerului de chei VPN. *8400* - Eșuare 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 distanță. *8408* - E expirat timpul de negocieri de conexiune VPN ale managerului de chei VPN. *8500 sau 8509* - A apărut o eroare de rețea la managerul de chei VPN.

Recuperare

1. Verificați istoricul de joburi pentru mesaje adiționale.
2. Corecți erorile și încercați cererea din nou.
3. Folosiți Navigator iSeries pentru a verifica sau corecta configurația de politică VPN. Asigurați-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.

TCP8608 Conexiunea VPN, [*nume conexiune*], nu a putut obține o adresă NAT

Acest grup de chei dinamice sau conexiune de date au specificat că translatarea de adresă rețea (NAT) e făcută pe una sau mai multe adrese și că a eșuat datorită unuia dintre posibilele coduri motiv: *1* - Adresa căruia trebuie să i se aplice NAT nu este o adresă IP singulară. *2* - Toate adresele disponibile au fost folosite.

1. Verificați istoricul de joburi pentru mesaje adiționale.
2. Corecți erorile și încercați cererea din nou.
3. Folosiți Navigator iSeries pentru a verifica sau corecta politica VPN. Asigurați-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. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Asigurați-vă că punctul final de conexiune local este definit și pornit folosind comanda NETSTAT OPTION(*IFC).
3. Corecți orice erori și încercați cererea din nou.

TCP8621 Punct final de date local nedisponibil

Nu s-a putut activa această conexiune VPN pentru că punctul final de date local nu a fost disponibil.

1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Asigurați-vă că punctul final de conexiune local este definit și pornit folosind comanda NETSTAT OPTION(*IFC).
3. Corecți orice erori și încercați cererea din nou.

Mesajele de eroare ale managerului de conexiune VPN

| Mesaj | Cauză | Recuperare |
|---|---|--|
| 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 și această conexiune este definită ca un gateway de securitate. | <ol style="list-style-type: none">1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.2. Folosiți Navigator iSeries pentru a schimba politica VPN asociată cu această conexiune VPN.3. Corectăți orice erori și încercați cererea din nou. |
| TCP8623 Conexiunea VPN se suprapune 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 [<i>valoarea punctului final de date local</i>] și un punct final de date la distanță de [<i>valoarea punctului final de date la distanță</i>]. | <ol style="list-style-type: none">1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.2. Folosiți Navigator iSeries pentru a vizualiza toate conexiunile activate care au puncte finale de date locale și puncte finale de date la distanță care se suprapun peste conexiune. Schimbați politica unei conexiuni existente dacă amândouă conexiunile sunt necesare.3. Corectăți orice erori și încercați 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. | <ol style="list-style-type: none">1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.2. Folosiți Navigator iSeries pentru a afișa restricțiile de punct 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 verificați punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acțiune IPSEC și un nume de conexiune VPN asociat cu această conexiune. Schimbați politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune.3. Corectăți orice erori și încercați cererea din nou. |
| TCP8625 Conexiunea VPN e eșuat la o verificare de algoritm ESP | Nu s-a putut activa această conexiune VPN din cauza insuficienței cheii secrete asociată cu conexiunea. | <ol style="list-style-type: none">1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.2. Folosiți Navigator iSeries pentru a afișa politica asociată cu această conexiune și introduceți o cheie secretă diferită.3. Corectăți orice erori și încercați cererea din nou. |

Mesajele de eroare ale managerului de conexiune VPN

Mesaj

TCP8626 Punctul final al conexiunii VPN nu este același cu punctul final de date.

Cauză

Nu s-a putut activa această conexiune VPN pentru că politica specifică o gazdă existentă și punctul final de conexiune VPN nu este același lucru cu punctul final de date.

Recuperare

1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Folosiți Navigator iSeries pentru a afișa restricțiile de punct 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 verificați punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acțiune IPSEC și un nume de conexiune VPN asociat cu această conexiune. Schimbați politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune.
3. Corectați orice erori și încercați cererea din nou.

TCP8628 Regula de filtrare politici nu este încărcată

Regula de filtrare politici pentru această conexiune nu este activă.

1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Folosiți Navigator iSeries pentru a afișa filtrele de politici active. Verificați regula de filtrare politici pentru această conexiune.
3. Corectați orice erori și încercați cererea din nou.

TCP8629 Pachet IP abandonat pentru conexiunea VPN

Această conexiune VPN are VPN NAT configurat și setul cerut de adrese NAT a depășit adresele disponibile NAT.

1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Folosiți Navigator iSeries pentru a crește numărul de adrese NAT atribuite pentru această conexiune VPN.
3. Corectați orice erori și încercați cererea din nou.

TCP862A Conexiunea PPP nu a putut să pornească

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 eșuare a apărut.

1. Verificați istoricele de joburi pentru mesaje adiționale de aplicat acestei conexiuni.
2. Verificați istoricul de joburi asociat cu conexiunea PPP.
3. Corectați orice erori și încercați cererea din nou.

Operații înrudite

“Vizualizarea atributelor conexiunilor active” la pagina 52

Finalizați această operație pentru a verifica starea și alte atribute ale conexiunilor dumneavoastră active.

Depanarea VPN cu urmărirea comunicațiilor

IBM i5/OS furnizează capabilitatea de urmărire a datelor pe o linie de comunicație, cum ar fi o interfață rețea locală (LAN) sau rețea pe zonă extinsă (WAN). Utilizatorul mijlociu poate să nu înțeleagă întregul conținut al datelor de urmărire. Oricum, puteți folosi intrările de urmărire pentru a determina dacă un schimb de date între sistemele la distanță și local a avut loc.

Pornirea urmăririi de comunicații

Folosiți comanda de pornire urmărire comunicații (STRCMNTRC) pentru a porni urmărirea de comunicații 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 explicați în lista următoare:

CFGOBJ (Obiectul de configurare)

Numele obiectului de configurație de urmărit. Obiectul este fie o descriere de linie, de interfață rețea sau de server rețea.

CFGTYPE (Tip de configurare)

E urmărită o linie (*LIN), o interfață rețea (*NWI) sau un server de rețea (*NWS).

MAXSTG (Dimensiune buffer)

Dimensiunea buffer-ului necesar urmăririi. Valoarea implicită este setată la 128 KB. Intervalul merge de la 128 KB la 64 MB. Dimensiunea maximă actuală a buffer-ului pe întreg sistemul este definită în Uneltele de service sistem (SST). De aceea, puteți primi un mesaj de eroare când se folosește o dimensiune de buffer mai mare la comanda STRCMNTRC, decât cea definită în SST. Țineți minte că suma dimensiunilor de buffer specificate pe toate urmărirea de comunicații pornite nu trebuie să depășească dimensiunea maximă de buffer definită în SST.

DTADIR (Direcția datelor)

Direcția traficului de date de urmărit. Direcția poate fi doar trafic de ieșire (*SND), doar trafic de intrare (*RCV) sau ambele (*BOTH).

TRCFULL (Urmă plină)

Ce apare când buffer-ul 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 îmbrobodește 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 buffer-ul de urmărire, specificat în parametrul MAXSTG, este plin de înregistrări de urmărire. Ca o regulă generală, mereu să definiți dimensiunea buffer-ului astfel încât să fie suficient de mare ca să rețină toate înregistrările de urmărire. Dacă urmărirea se derulează la început, puteți pierde informații importante de urmărire. Dacă experimentați o problemă de intermitență înaltă, definiți buffer-ul de urmărire să fie destul de mare astfel ca o derulare a buffer-ului să nu abandoneze informații importante.

USRDTA (Numărul de octeți utilizator de urmărit)

Definește numărul de date de urmărit în partea de date utilizator a cadrelor de date. Implicit doar primii 100 de octeți de date utilizator sunt capturate pentru interfețele LAN. Pentru toate celelalte interfețe, toate datele utilizator sunt capturate. Asigurați-vă că specificați *MAX dacă suspectați probleme în datele utilizator a unui cadru.

TEXT (Descriere urmărire)

Furnizează o descriere cu sens a urmăririi.

Oprirea urmării de comunicații

Dacă nu specificați altfel, urmărirea se oprește tipic în momentul în care apare condiția pe care o urmăriți. Folosiți comanda de terminare urmărirea de comunicații (ENDCMNTRC) pentru a opri urmărirea. Următoarea comandă este un exemplu de comandă ENDCMNTRC:

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

Comanda are doi parametri:

CFGOBJ (Obiectul de configurare)

Numele obiectului de configurare pentru care urmărirea rulează. Obiectul este fie o descriere de linie, de interfață rețea sau de server rețea.

CFGTYPE (Tip de configurare)

E urmărită o linie (*LIN), o interfață rețea (*NWI) sau un server de rețea (*NWS).

Tipărirea datelor de urmărire

După ce ați oprit urmărirea de comunicații, trebuie să tipăriți datele de urmărire. Folosiți comanda de tipărire a urmărirea de comunicații (PRTCMNTRC) pentru a executa această operație. Atât timp cât tot traficul de linie este capturat în perioada de urmărire, aveți opțiuni de filtrare multiple pentru generarea ieșirii. Încercați să păstrați fișierul spool pe cât de mic posibil. Acesta face analiza mai repede și mai eficient. În cazul unei probleme VPN, filtrați doar în traficul IP și, dacă e posibil, într-o adresă IP specifică. Aveți opțiunea de filtrare pe un număr de port IP anume. Ceea ce urmează este un exemplu de comandă PRTCMNTRC:

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

În acest exemplu, urmărirea este formatată pentru trafic IP și conține doar date pentru adresa IP, unde adresa sursă și destinație este 10.50.21.1 și numărul de port IP destinație sau sursă este 500.

Doar cei mai importanți parametri ai comenzii pentru analizarea de probleme VPN, sunt explicați mai jos:

CFGOBJ (Obiectul de configurare)

Numele obiectului de configurare pentru care urmărirea rulează. Obiectul este fie o descriere de linie, de interfață rețea sau de server rețea.

CFGTYPE (Tip de configurare)

E urmărită o linie (*LIN), o interfață rețea (*NWI) sau un server de rețea (*NWS).

FMTTCP (Format de date TCP/IP)

Dacă se formatează urmărirea pentru datele TCP/IP și UDP/IP. Specificați *YES pentru a formata urmărirea pentru datele IP.

TCPIPADR (Formatul de date TCP/IP după adresă)

Acest parametru conține două elemente. Dacă specificați adresele IP pe fiecare element, doar traficul IP între acele adrese vor tipări.

SLTPORT (Număr de port IP)

Numărul de port IP de filtrat.

FMTBCD (Format de date broadcast)

Dacă toate cadrele de broadcast sunt tipărite. Valoarea implicită este Da. Dacă nu doriți, de exemplu, cererile ARP (Address Resolution Protocol) specificați *NO; altfel puteți fi copleșit cu mesaje de tip broadcast.

Operații înrudite

“Inițierea în depanarea VPN” la pagina 54

Vedeți aceste informații pentru a începe găsirea și corectarea problemelor de conexiune VPN.

Informații înrudite pentru VPN

Folosiți acest subiect pentru a găsi alte surse de informații despre VPN și subiecte înrudite.

Pentru mai multe scenarii și descrieri de configurații VPN, consultați aceste surse de informații:

- OS/400 V5R2 Virtual Private Networks: Remote Access to the IBM eServer iSeries Server with Windows 2000

VPN Clients, REDP0153 

Această carte IBM Redbook oferă un proces pas cu pas pentru configurarea tunelului VPN folosind VPN din i5/OS și VPN suportul L2TP și IPSec integrat în Windows 2000.

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

Acest manual explorează conceptele VPN și descrie implementarea folosind securitate IP (IPSec) și Layer 2 Tunneling Protocol (L2TP).

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

Acest manual explorează toate caracteristicile de securitate integrată disponibile pe sistemul de operare iSeries cum ar fi filtre IP, NAT, VPN, server proxy HTTP, SSL, DNS, releu poștă, auditare și înregistrare în istoric. Descrie utilizarea lor prin exemple practice.

- Virtual Private Networking: Securing Connections 

Această pagină Web conține știri recente despre VPN, liste cu cele mai noi PTF-uri și legături la alte site-uri de interes.

- Alte subiecte și cărți Redbook legate de securitate

Mergeți aici pentru o listă de informații legate de securitate disponibile online.

Salvarea fișierelor PDF

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

1. Faceți clic dreapta pe PDF în browser (faceți clic dreapta pe legătura de mai sus).
2. Faceți clic pe **Save Target As...** dacă folosiți Internet Explorer. Faceți clic pe **Save Link As** dacă folosiți Netscape Communicator.
3. Navigați la directorul în care doriți să salvați fișierul PDF.
4. Faceți clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

Aveți nevoie de Acrobat Reader pentru a vedea sau tipări aceste PDF-uri. Puteți descărca o copie de pe site-ul Web

Adobe (www.adobe.com/products/acrobat/readstep.html) .

Anexa. Observații

Această publicație a fost elaborată pentru produse și servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Luați legătura cu reprezentanța IBM locală pentru a obține informații cu privire la produsele și 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 funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea și verificarea modului în care funcționează un produs, program sau serviciu non-IBM ține de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Furnizarea acestui document nu vă acordă nici o licență asupra acestor patente. Puteți trimite întrebări cu privire la licențe, în scris, la:

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

Pentru întrebări privind licența pentru informațiile DBCS (double-byte character set), contactați departamentul de proprietate intelectuală al IBM-ului din țara dumneavoastră sau trimiteți întrebările în scris la:

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

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor țări unde asemenea prevederi sunt incompatibile cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANȚIE EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE CU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilității pentru garanțiile exprese sau deduse în anumite tranzacții, de aceea este posibil ca această declarație să nu fie valabilă în cazul dumneavoastră.

Aceste informații pot include inexactități tehnice sau erori tipografice. Se efectuează modificări periodice la informațiile incluse aici; aceste modificări vor fi încorporate în noi ediții ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment, fără notificare.

Referirile din aceste informații la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezența 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 informațiile pe care le furnizați, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație pentru dumneavoastră.

Posesorii de licență pentru acest program care doresc să obțină informații despre el cu scopul de a realiza: (i) schimbul de informații între programe create independent și alte programe (inclusiv acesta) și (ii) utilizarea mutuală a informațiilor care au fost schimbate, trebuie să contacteze:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informații pot fi făcute disponibile în conformitate cu anumiți termeni și condiții, iar în unele cazuri după plata unei taxe.

- | Programul cu licență descris în aceste informații și toate materialele cu licență disponibile pentru acesta sunt furnizate
- | de către IBM conform termenilor din Contractul IBM cu Clientul, Contractul de Licență IBM pentru Programele
- | Internaționale, Contractul de Licență IBM pentru Codul Mașină, sau orice contract echivalent dintre noi.

Datele de performanță prezentate aici au fost determinate într-un mediu controlat. De aceea, rezultatele obținute în alte medii de operare pot varia semnificativ. Anumite măsurători s-ar putea să fi fost făcute pe sisteme în faza de dezvoltare și nu este nici o garanție că aceste măsurători vor da aceleași rezultate pe sistemele disponibile pe piață. 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.

Informațiile privind produsele non-IBM au fost obținute de la furnizorii acestor produse, din anunțurile lor publicate sau din alte surse publice. IBM nu a testat aceste produse și nu poate confirma nivelul performanței, compatibilității sau al oricăror altor pretense calități legate de produsele non-IBM. Întrebările legate de capacitățile produselor non-IBM trebuie să fie adresate furnizorilor acestor produse.

Toate declarațiile referitoare la direcția sau intențiile viitoare ale IBM pot fi modificate sau retrase fără notificare, ele reprezentând doar niște obiective.

Toate prețurile IBM afișate sunt prețuri de vânzare cu amănuntul sugerate de IBM; ele reprezintă valori curente și pot fi modificate fără notificare. Prețurile dealer-ilor pot varia.

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

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

LICENȚĂ DE COPYRIGHT:

Aceste informații cuprind exemple de programe de aplicație în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteți copia, modifica și distribui aceste programe-eșantion în orice formă fără necesitatea unei plăți către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicație în concordanță cu interfața de programare a aplicației pentru platforma de operare pentru care sunt scrise programele-eșantion. Aceste exemple nu au fost testate complet în toate condițiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcționale.

Fiecare copie sau orice porțiune din aceste programe-eșantion sau orice lucrare derivată trebuie să includă un aviz de copyright, după cum urmează:

© (numele companiei dumneavoastră) (anul). Porțiuni din acest cod sunt derivate din Programe eșantion ale IBM Corp.
© Copyright IBM Corp. _introduceți anul sau anii_. Toate drepturile rezervate.

Dacă vedeți aceste informații folosind o copie electronică, fotografiile și ilustrațiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale deținute de International Business Machines Corporation în Statele Unite, în alte țări sau ambele:

- | AS/400
- | eServer
- | i5/OS
- | IBM
- | iSeries
- | OS/400
- | SAA

- | Intel, Intel Inside (logo-uri), MMX și Pentium sunt mărci comerciale ale Intel Corporation în Statele Unite, în alte țări sau în ambele.

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci înregistrate deținute de Microsoft Corporation în Statele Unite, în alte țări sau ambele.

UNIX este o marcă comercială înregistrată deținută de The Open Group în Statele Unite și în alte țări.

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

Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

Utilizare personală: Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza lucrări derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

Utilizare comercială: Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit de la IBM.

În afara celor acordate expres prin această permisiune, nu se acordă nici o altă permisiune, licență sau drept, explicite sau implicite, pentru aceste publicații sau orice informații, date, software sau alte elemente pe care le conțin și care reprezintă o proprietate intelectuală.

IBM își păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreția sa, dacă folosirea publicațiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât în deplină conformitate cu legile și regulamentele aplicabile, inclusiv toate legile și regulamentele de export ale Statelor Unite.

IBM NU OFERĂ GARANȚII DESPRE CONȚINUTUL ACESTOR PUBLICAȚII. PUBLICAȚIILE SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.



Tipărit în S.U.A.