System i

Securitate
Reţea privată virtuală

Versiunea 6 Ediţia 1

System i

Securitate
Reţea privată virtuală

Versiunea 6 Ediţia 1

Notă

Înainte de a utiliza aceste informaţii şi produsul pe care îl suportă, citiţi informaţiile din “Observaţii”, la pagina 79.

Această ediţie se aplică versiunii 6, ediţia 1, modificarea 0 a IBM i5/OS (număr de produs 5761-SS1) şi tuturor ediţiilor şi modificărilor care vor urma până când nu se indică altfel în ediţii noi. Această versiune nu rulează pe toate modelele RISC (reduced instruction set computer), nici pe modelele CISC.

Cuprins

Reţea privată virtuală

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

VPN este o componentă care poate fi instalată opţional din System i Navigator, interfaţa grafică cu utilizatorul (GUI) pentru i5/OS. Ea vă permite să creaţi o cale sigură capăt-la-capăt pentru orice combinaţie de gazdă şi gateway. VPN foloseşte metode de autentificare, algoritmi de criptare şi alte măsuri de precauţie pentru ca datele trimise între cele două puncte ale conexiunii să rămână sigure.

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

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

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

Ce este nou pentru V6R1

Citiţi despre informaţii noi sau modificate semnificativ pentru colecţia de subiecte Reţea privată virtuală.

Funcţie nouă: IP versiunea 6

Acum puteţi folosi IP versiunea 6 pentru a crea un VPN cu următoarele tipuri de conexiune: gazdă-la-gazdă, gazdă-la-gateway şi gateway-la-gateway. Conexiunile VPN suportă IP versiunea 6 pentru adresă, interval, subreţea şi nume gazdă. Toţi vrăjitorii VPN au fost actualizaţi să accepte noile tipuri de ID IP versiunea 6.

- Protocol Internet (IP) versiunea 6

Cum puteţi vedea ce este nou sau modificat

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

- Imaginea » pentru marcarea locului unde încep informaţiile noi sau cele modificate.
- Imaginea « pentru marcarea locului unde se termină informaţiile noi sau cele modificate.

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

Fişier PDF pentru reţea privată virtuală (VPN)

Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

Pentru a vizuailza sau descărca versiunea PDF a acestui document, selectaţi VPN (Virtual private network) (aproximativ 1100KB).

Salvarea fişierelor PDF

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

1. Faceţi clic dreapta pe legătura la PDF din acest browser.
2. Faceţi clic pe **Save Target As...** dacă folosiţi Internet Explorer. Faceţi clic pe **Save Link As** dacă folosiţi Netscape Communicator.
3. Navigaţi la directorul în care doriţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

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

Conceptele VPN

Este important să aveţi cel puţin cunoştinţe de bază despre tehnologii standard VPN înainte de a implementa o conexiune VPN.

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

Protocoale de securitate IP

IPSec (IP Security) oferă o bază stabilă şi de lungă durată pentru furnizarea securităţii nivelului reţea.

IPSec suportă toţi algoritmii de criptare folosiţi în prezent şi poate de asemenea îngloba algoritmi noi şi mai puternici pe măsură ce aceştia apar. Protocoalele IPSec tratează aceste probleme majore de securitate:

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

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

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

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

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

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

Notă: Unele configuraţii VPN pot avea un punct vulnerabil din punct de vedere securitate, în funcţie de cum este configurat IPSec. Vulnerabilitatea afectează configuraţiile unde IPsec este configurat să folosească EPS (Encapsulating Security Payload) în modul tunel cu confidenţialitate (criptare), dar fără protecţie de integritate (autentificare) sau AH (Authentication Header). Configuraţia implicită când este selectat ESP include întotdeauna un algoritm de autentificare care oferă protecţia la integritate. De aceea, doar dacă algoritmul de

autentificare nu este înlăturat din transformarea ESP, configuraţiile VPN vor fi protejate împotriva acestei vulnerabilităţi. Configuraţia VPN IBM Universal Connection nu este afectată de această vulnerabilitate.

Pentru a verifica dacă sistemul este afectat de această vulnerabilitate de securitate, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Politici de securitate IP → Politici de date** .
2. Faceţi clic dreapta pe politica de date pe care vreţi să o verificaţi şi selectaţi **Proprietăţi**.
3. Faceţi clic pe fişa **Propuneri**.
4. Selectaţi orice propunere de protecţie de date care foloseşte protocolul ESP şi faceţi clic pe **Editare**.
5. Faceţi clic pe fişa **Transformări**.
6. Selectaţi orice transformare din listă care foloseşte protocolul ESP şi faceţi clic pe **Editare**.
7. Verificaţi că algoritmul de autentificare are orice altă valoare decât **Fără**.

Internet Engineering Task Force (IETF) defineşte formal IPSec în RFC 2401, *Security Architecture for the Internet Protocol*. Puteţi 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 comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.

Informaţii înrudite

http://www.rfc-editor.org

Authentication Header

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

AH asigură integritatea datelor cu suma de control pe care o generează un cod de autentificare mesaj, cum este MD5. Pentru a asigura autentificarea originii datelor, AH include o cheie partajată secretă în algoritmul pe care îl foloseşte pentru autentificare. Pentru a asigura protecţia la redare, AH foloseşte un câmp de numere de ordine din cadrul antetului AH. Aici nu are nici o importanţă că aceste trei funcţii distincte sunt deseori folosite împreună şi referite ca autentificare. În termeni mai simpli, AH asigură că datele dumneavoastră nu au fost modificate pe ruta către destinaţia finală.

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

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

Moduri de folosire a AH

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

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

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

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

De ce AH?

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

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

Folosirea ESN cu AH

Dacă folosiţi protocolul AH atunci puteţi dori să activaţi ESN (Extended Sequence Number). ESN vă permite să transmiteţi volume mari de date la o viteză mare fără să fie necesară retransmiterea cheilor (re-keying). Conexiunea VPN foloseşte numere de ordine pe 64 de biţi în locul numerelor pe 32 de biţi peste IPSec. Folosind numere de ordine de 64 de biţi permite mai mult timp înainte de retransmiterea cheilor, care împiedică epuizarea şi minimizarea folosirii resurselor de sistem.

Ce algoritmi foloseşte AH pentru a-mi proteja informaţiile?

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

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

Concepte înrudite

“Encapsulating Security Payload”
Protocolul Encapsulating Security Payload (ESP) furnizează confidenţialitatea datelor şi, opţional, autentificarea originii datelor, verificarea integrităţii datelor şi protecţie la redare.

Informaţii înrudite

http://www.rfc-editor.org

Encapsulating Security Payload

Protocolul Encapsulating Security Payload (ESP) furnizează confidenţialitatea datelor şi, opţional, autentificarea originii datelor, verificarea integrităţii datelor şi protecţie la redare.

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

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

Două moduri de a folosi ESP

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

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

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

Ce algoritmi foloseşte ESP pentru a proteja informaţiile?

ESP foloseşte o cheie simetrică, cu care ambele părţi criptează şi decriptează datele pe care le schimbă. Transmiţătorul şi receptorul trebuie să se înţeleagă asupra cheii înainte de a putea comunica în siguranţă. VPN utilizează DES (Data Encryption Standard), 3DES (triplu-DES), RC5, RC4 şi AES (Advanced Encryption Standard) pentru criptare.

Dacă alegeţi algoritmul AES, atunci puteţi dori să activaţi ESN (Extended Sequence Number). ESN vă permite să transmiteţi volume mari de date la o viteză mare. Conexiunea VPN foloseşte numere de ordine pe 64 de biţi în locul numerelor pe 32 de biţi peste IPSec. Folosind numere de ordine de 64 de biţi permite mai mult timp înainte de retransmiterea cheilor, care împiedică epuizarea şi minimizarea folosirii resurselor de sistem.

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

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

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

Concepte înrudite

“Authentication Header” la pagina 3
Protocolul Authentication Header (AH) furnizează autentificarea originii datelor, integritatea datelor şi protecţie la redare. Totuşi, AH nu oferă confidenţialitatea datelor, ceea ce înseamnă că toate datele dumneavoastră sunt trimise transparent.

Informaţii înrudite

http://www.rfc-editor.org

AH şi ESP combinate

VPN vă permite să combinaţi AH şi ESP pentru conexiuni gazdă-la-gazdă în modul transport.

Combinarea acestor protocoale protejează întreaga datagramă IP. Deşi combinarea celor două protocoale oferă mai multă securitate, supra-procesarea implicată s-ar putea să fie prea mare decât beneficiile aduse.

Gestionarea cheilor

Un VPN dinamic furnizează securitate suplimentară pentru comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.

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

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

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

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

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

Fazele gestionării cheilor

Managerul de chei VPN foloseşte două faze distincte în implementare.

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

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

Autentificarea cu *Semnătură RSA* oferă o securitate mai mare decât cheile prepartajate deoarece acest mod foloseşte certificate digitale pentru a furniza autentificarea. Trebuie să vă configuraţi certificatele digitale prin utilizarea DCM-ului (Digital Certificate Manager). În plus, unele soluţii 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 folosiţi trebuie să provină de la autorităţi de certificare în care au încredere ambele servere.

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

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

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

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

Lecturi recomandate

Dacă vreţi să citiţi mai multe despre protocolul IKE (Internet Key Exchange) şi despre gestiunea cheie, revedeţi aceste cereri pentru comentarii (RFC) IETF (Internet Engineering Task Force):

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

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

Concepte înrudite

“Scenariu: VPN prietenos pentru firewall-uri” la pagina 28
În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago şi o gazdă din Minneapolis, atunci când amândouă serverele sunt în spatele unui firewall.

“Protocoale de securitate IP” la pagina 2
IPSec (IP Security) oferă o bază stabilă şi de lungă durată pentru furnizarea securităţii nivelului reţea.

Operaţii înrudite

“Configurarea unei politici Schimbare de chei Internet (IKE)” la pagina 47
Politica IKE (Internet Key Exchange) defineşte ce nivel de protecţie de autentificare şi criptare foloseşte IKE în faza 1 a negocierilor.

“Configurarea unei politici de date” la pagina 48
O politică de date defineşte ce nivel de autentificare sau criptare protejează datele care circulă prin VPN.

Informaţii înrudite

http://www.rfc-editor.org

Layer 2 Tunnel Protocol

Conexiunile L2TP (Layer 2 Tunneling Protocol), care mai sunt numite linii virtuale, furnizează acces eficient utilizatorilor la distanţă prin permiterea unei reţele de sisteme comune să gestioneze adresele IP asignate utilizatorilor la distanţă. Mai mult, conexiunile L2TP furnizează acces sigur la sistemul sau reţeaua dumneavoastră când le folosiţi împreună cu IP Security (IPSec).

L2TP suportă două felluri de tunel: tunelul voluntar şi tunelul obligatoriu. Diferenţa majoră dintre aceste două moduri de tunel este punctul final. La tunelul voluntar, tunelul se termină la clientul la distanţă în timp ce tunelul obligatoriu se termină la ISP (Internet Service Provider).

La un **tunel obligatoriu** L2TP, o gazdă la distanţă iniţiază o conexiune cu ISP-ul acesteia. Apoi ISP-ul stabileşte o conexiune L2TP între utilizatorul la distanţă şi reţeaua companiei. Deşi ISP stabileşte conexiunea, dumneavoastră decideţi cum să protejaţi traficul folosind VPN. Pentru un tunel obligatoriu, ISP-ul trebuie să suporte LT2P.

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

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

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

Concepte înrudite

“Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec” la pagina 22
În acest scenariu, aflaţi cum să setaţi o conexiune între o gazdă a filialei şi sediul central care foloseşte L2TP protejat de IPSec. Biroul filialei are o adresă IP alocată dinamic, în timp ce biroul companiei are o adresă IP statică, rutabilă global.

Translatarea adreselor de reţea pentru VPN

VPN furnizează un mijloc pentru efectuarea de translatare a adreselor de reţea, denumit VPN NAT. VPN NAT diferă de NAT tradiţional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE şi IPSec. Studiaţi acest subiect pentru a afla mai multe.

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

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

Notă: În prezent FTP nu suportă VPN NAT.

Cum ar trebui să folosesc VPN NAT?

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

VPN NAT pentru prevenirea conflictelor între adresele IP

Acest tip de VPN NAT vă permite să evitaţi posibile conflicte între adrese IP când configuraţi o conexiune VPN între reţele sau sisteme cu scheme de adresare similare. Un scenariu tipic este cel în care ambele companii doresc să creeze conexiuni VPN prin folosirea unuia dintre intervalele de adrese IP private atribuite lor. De exemplu, 10.*.*.*. Cum configuraţi acest tip de VPN NAT depinde de sistemul dumneavoastră, dacă este iniţiatorul sau respondentul pentru conexiunea VPN. Când sistemul dumneavoastră este iniţiatorul conexiunii, vă puteţi translata adresele locală în unele care sunt compatibile cu adresa partenerului din conexiunea VPN. Când sistemul dumneavoastră este

respondentului conexiunii, puteţi translata adresele la distanţă ale partenerului VPN în unele care sunt compatibile cu schema dumneavoastră de adrese locale. Configuraţi acest tip de translatare de adrese doar pentru conexiunile dumneavoastră dinamice.

VPN NAT pentru ascunderea adreselor locale

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

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

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

Scenariul, Folosire translatare adresă de reţea pentru VPN vă oferă un exemplu despre cum să configuraţi VPN NAT pentru a ascunde adrese locale în modelul System i.

Pentru instrucţiuni pas-cu-pas despre cum să setaţi VPN NAT pe sistemul dumneavoastră, folosiţi ajutorul online disponibil în interfaţa VPN din System i Navigator.

Concepte înrudite

"Scenariu: Folosire translatare adresă de reţea pentru VPN" la pagina 39
În acest scenariu, compania dumneavoastră vrea să schimbe date confidenţiale cu unul dintre partenerii ei de afaceri utilizând VPN. Pentru a proteja şi mai mult structura reţelei, compania dumneavoastră va folosi de asemenea VPN NAT, pentru a ascunde adresa IP privată a sistemului pe care îl foloseşte pentru a găzdui aplicaţiile la care are acces partenerul de afaceri.

"Fişă de lucru pentru planificare pentru conexiuni manuale" la pagina 44
Completaţi această fişă de lucru înainte de a configura o conexiune manuală.

IPSec compatibil NAT cu UDP

Încapsularea UDP permite traficului IPSec să treacă printr-un dispozitiv NAT convenţional. Treceţi în revistă acest subiect pentru mai multe informaţii despre ce este şi de ce ar trebui să îl folosiţi pentru conexiunile dumneavoastră VPN.

Problema: NAT-ul convenţional întrerupe VPN-ul

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

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

Soluţia: Încapsularea UDP

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

Puteţi să aplicaţi încapsularea UDP doar la VPN-uri care vor folosi IPSec ESP în modul tunel sau modul transport. În plus, sistemul se poate comporta doar ca un client pentru încapsulare UDP. Cu alte cuvinte, poate doar să *iniţieze* trafic încapsulat UDP.

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

Datagrama IPv4 originală:

După aplicarea IPSec ESP în modul tunel:

După ce se aplică Încapsularea UDP:

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

Datagrama IPv4 originală:

După aplicarea IPSec ESP în modul transport:

După ce se aplică Încapsularea UDP:

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

Concepte înrudite

"Scenariu: VPN prietenos pentru firewall-uri" la pagina 28
În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago şi o gazdă din Minneapolis, atunci când amândouă serverele sunt în spatele unui firewall.

Compresie IP

Protocolul IP Payload Compression (IPComp) reduce dimensiunea datagramelor IP comprimând datagramele pentru a creşte performanţa comunicaţiei între doi parteneri.

Intenţia este să se mărească performanţa totală a comunicaţiei atunci când comunicaţia se face peste legături lente sau încăcate. IPComp nu furnizează nici un fel de securitate şi trebuie folosit cu o transformare AH sau ESP când comunicaţia are loc peste o conexiune VPN.

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

Informaţii înrudite

http://www.rfc-editor.org

VPN şi filtrarea IP

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

Cele mai multe conexiuni VPN necesită reguli filtru pentru a funcţiona corect. Regulile de filtrare necesare depind de tipul de conexiune VPN pe care o configuraţi, ca şi de tipul ce trafic pe care doriţi să-l controlaţi. În general, fiecare conexiune va avea un filtru de politică. Filtrul de politică defineşte care adrese, protocoale şi porturi pot folosi VPN-ul. În plus, conexiunile care suportă protocolul IKE (Internet Key Exchange) au tipic reguli care sunt scrise explicit pentru a permite procesare IKE asupra conexiunii. VPN poate genera aceste reguli automat. Când este posibil, permiteţi VPN-ului să genereze filtrele de politică pentru dumneavoastră. Aceasta nu va ajuta doar la eliminarea erorilor, dar elimină de asemenea şi nevoia ca dumneavoastră să configuraţi regulile ca un pas separat, folosind editorul Reguli pachet din System i Navigator.

Desigur, sunt şi excepţii. Examinaţi aceste subiecte pentru a afla mai multe despre alte, mai puţin obişnuite, VPN-uri şi tehnici şi concepte de filtrare care s-ar putea aplica în situaţia dumneavoastră particulară:

Concepte înrudite

"Configurare reguli pachet VPN" la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Conexiuni VPN fără filtre de politici

În cazul în care punctele finale ale conexiunii dumneavoastră VPN sunt adrese IP specifice, singulare şi doriţi să porniţi VPN fără a fi nevoie să scrieţi sau să activaţi reguli de filtrare pe sistem, puteţi configura un filtru de politică dinamic.

O regulă de filtrare politică defineşte care adrese, protocoale şi porturi pot utiliza un VPN şi dirijează traficul corespunzător prin conexiune. În unele cazuri, s-ar putea să doriţi să configuraţi o conexiune care nu necesită o regulă de filtrare politici. De exemplu, s-ar putea să aveţi reguli de pachet non-VPN încărcate în interfaţa pe care conexiunea dumneavoastră VPN o va folosi, astfel că mai degrabă decât să dezactivaţi regulile active din acea interfaţă, vă decideţi să configuraţi VPN-ul astfel încât sistemul dumneavoastră să gestioneze dinamic toate filtrele pentru conexiune. Filtrul de politici pentru acest tip de conexiune este denumit **filtrul de politici dinamic**. Înainte să puteţi folosi un filtru dinamic de politici pentru conexiunea dumneavoastră VPN, trebuie să fie adevărate următoarele:

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

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

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

IKE Implicit

Pentru ca negocierile IKE (Internet Key Exchange) să aibă loc pentru VPN-ul dumneavoastră, trebuie să permiteţi datagrame UDP prin 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, majoritatea VPN-urilor necesită ca negocieri IKE să aibă loc înainte de procesarea IPSec. IKE foloseşte binecunoscutul port 500, astfel că pentru ca IKE să funcţioneze bine, trebuie să permiteţi datagramele UDP pe port 500 pentru acest tip de trafic IP. Dacă nu există reguli de filtrare special pentru permiterea traficului IKE, atunci acesta este implicit permis. Totuşi, regulile scrise specific pentru traficul portului 500 UDP sunt tratate pe baza a ceea ce e definit în regulile filtru active.

Scenarii: VPN

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

Concepte înrudite

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

Informaţii 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 aceste scenariu, compania dumneavoastră doreşte să stabilească un VPN între subreţelele a două departamente aflate la distanţă prin intermediul unei perechi de modele System i cu rolul de gateway-uri VPN.

Situaţie

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

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

Important: Acest scenariu arată modelul System i de gateway-uri de securitate ataşate direct la Internet. Absenţa unui firewall are intenţia de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile de securitate implicate de fiecare dată când vă conectaţi la Internet.

Avantaje

Acest scenariu are următoarele avantaje:

- Folosirea Internetului sau a unui intranet existent reduce costul liniilor private între subreţele la distanţă.
- Folosirea Internetului sau a unui intranet existent reduce complexitatea instalării şi întreţinerii liniilor private şi a echipamentului asociat.
- Folosirea Internetului permite locaţiilor la distanţă să se conecteze aproape oriunde în lume.
- Folosirea VPN furnizează utilizatorilor acces la toate sistemele şi resursele de pe ambele părţi ale conexiunii ca şi cum ar fi conectate printr-o conexiune cu linie închiriată sau WAN (wide area network).
- Folosirea metodelor standard de autentificare şi de criptare asigură securitatea informaţiilor sensibile, trimise de la o locaţie la alta.
- Schimbându-vă cheile de criptare dinamic şi în mod regulat, se simplifică instalarea şi se minimizează riscul decodificării cheilor şi străpungerea securităţii.
- Utilizarea adreselor IP în fiecare subreţea la distanţă face nenecesară alocarea adreselor IP publice pentru fiecare client.

Obiective

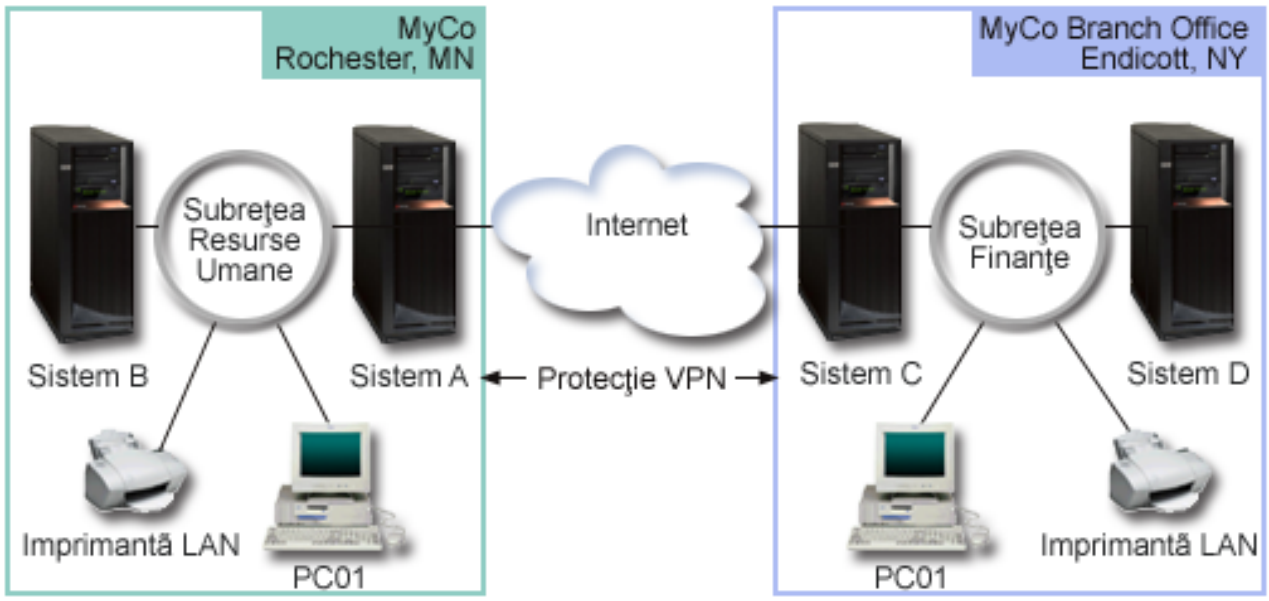
În acest scenariu, MyCo Inc. doreşte să stabilească un VPN între subreţelele departamentelor Resurse umane şi Finanţe printr-o pereche de modele System i. Ambele sisteme se vor comporta ca gateway-uri VPN. Într-o configuraţie VPN, un gateway gestionează cheile şi aplică IPSec datelor care se transmit prin tunel. Gateway-urile nu sunt punctele finale de date ale conexiunii.

Obiectivele acestui scenariu sunt următoarele:

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

Detalii

Următoarea ilustraţie prezintă caracteristicile reţelei MyCo.



Departamentul Resurse Umane

- Sistem A rulează cu i5/OS Versiunea 5 Ediţia 3 (V5R3), sau mai nou, şi are rol de gateway VPN pentru Departamentul Resurse umane.
- Subreţeaua este 10.6.0.0 cu masca 255.255.0.0. Această subreţea reprezintă punctul final de date al tunelului VPN, la sediul MyCo Rochester.
- Sistem A se conectează la Internet cu adresa IP 204.146.18.227. Acesta este punctul final al conexiunii. Adică, Sistem A realizează gestionarea de chei şi aplică IPSec datagramelor IP de intrare şi ieşire.
- Sistem A se conectează la subreţeaua proprie cu adresa IP 10.6.11.1.
- Sistem B este un sistem de producţie din subreţeaua Resurse umane pe care rulează aplicaţii standard TCP/IP.

Departamentul Finanţe

- Sistem C rulează cu i5/OS Versiunea 5 Ediţia 3 (V5R3), sau mai nou, şi are rol de gateway VPN pentru Departamentul Finanţe.
- Subreţeaua este 10.196.8.0 cu masca 255.255.255.0. Această subreţea reprezintă punctul final de date al tunelului VPN, la sediul MyCo Endicott.
- Sistem C se conectează la Internet cu adresa IP 208.222.150.250. Acesta este punctul final al conexiunii. Adică, Sistem C realizează gestionarea de chei şi aplică IPSec datagramelor IP de intrare şi ieşire.
- Sistem C se conectează la subreţeaua proprie cu adresa IP 10.196.8.5.

Taskurile de configurare

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

Notă: Înainte de a porni aceste operaţii verificaţi rutarea TCP/IP pentru a vă asigura că cele două sisteme gateway pot comunica între ele prin Internet. În acest fel, vă asiguraţi că gazdele din fiecare subreţea rutează corespunzător către gateway-ul corespunzător pentru a accesa subreţeaua la distanţă.

Concepte înrudite

Rutarea TCP/IP şi echilibrarea încărcării

Informaţii înrudite

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

Completarea fişelor de lucru pentru planificare

Lista de verificare de planificare ilustrează tipul de informaţii de care aveţi nevoie înainte de a începe configurarea VPN-ului. Toate răspunsurile din lista de verificare a cerinţei preliminare trebuie să fie Da înainte de a continua cu setarea VPN.

Notă: Aceste fişe de lucru se aplică pentru Sistem A, repetaţi procesul pentru Sistem C, prin inversarea adreselor IP după nevoie.

Tabela 1. Cerinţe sistem

Listă de verificare pentru cerinţele preliminare	**Răspunsuri**
Sistemul rulează i5/OS V5R3, sau mai nou?	Da
Este instalată opţiunea Digital Certificate Manager?	Da
Este instalat System i Access pentru Windows?	Da
Este instalat System i Navigator?	Da
Este instalată subcomponenta Reţea din System i Navigator?	Da
Este instalat IBM TCP/IP Connectivity Utilities for i5/OS?	Da
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe sistem (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH şi ESP?	Da
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	Da

Tabela 2. Configuraţie VPN

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul	**Răspunsuri**
Ce tip de conexiune creaţi ?	gateway-la-gateway
Cum veţi denumi grupul de chei dinamice?	HRgw2FINgw
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja cheile?	echilibrate
Folosiţi 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 ?	Subreţea: 10.6.0.0 Mască: 255.255.0.0
Care este identificatorul serverului de chei la distanţă ?	Adresa IP: 208.222.150.250
Care este identificatorul punctului final de date la distanţă ?	Subreţea: 10.196.8.0 Mască: 255.255.255.0
Ce porturi şi protocoale doriţi să permiteţi prin conexiune ?	Oricare

Tabela 2. Configuraţie VPN (continuare)

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul	**Răspunsuri**
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja datele?	echilibrate
Pe care dintre interfeţe se aplică această conexiune ?	TRLINE

Configurarea VPN pentru Sistem A

Finalizaţi această operaţie pentru a configura Sistem A

Folosiţi următorii paşi şi informaţiile din fişele dumneavoastră de lucru pentru a configura VPN în Sistem A:

1. În System i Navigator, expandaţi **Sistem A → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune nouă.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi HRgw2FINgw.
6. Opţional: Specificaţi o descriere pentru acest grup de conexiuni.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gateway-ului dumneavoastră la alt gateway**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.
11. Apăsaţi pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectaţi **Nu** pentru a indica faptul că nu veţi folosi certificate pentru autentificarea conexiunii.
13. Apăsaţi **Următor** pentru a merge la pagina **Server de chei local**.
14. Selectaţi **Adresă IP Versiunea 4** din câmpul **Tip identificator**.
15. Selectaţi 204.146.18.227 din câmpul **Adresă IP**.
16. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
17. Selectaţi **Adresa IP Versiunea 4** din câmpul **Tip de identificator**.
18. Introduceţi 208.222.150.250 în câmpul **Identificator**.
19. Introduceţi topsecretstuff în câmpul **Cheie prepartajată**.
20. Apăsaţi **Următor** pentru a merge la pagina **Punct final local de date**.
21. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
22. Introduceţi 10.6.0.0 în câmpul **Identificator**.
23. Introduceţi 255.255.0.0 în câmpul **Mască subreţea**.
24. Apăsaţi **Următor** pentru a merge la pagina **Punct final de date distanţă**.
25. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
26. Introduceţi 10.196.8.0 în câmpul **Identificator**.
27. Introduceţi 255.255.255.0 în câmpul **Mască subreţea**.
28. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
29. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge în pagina **Politică de date**.
30. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.
31. Selectaţi **Folosirea algoritmului de criptare RC4**.
32. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
33. Selectaţi **TRLINE** din tabelul **Linie**.
34. Apăsaţi **Următor** pentru a merge la pagina **Sumar**. Revedeţi obiectele pe care le va crea pentru a asigura corectitudinea lor.

35. Apăsaţi pe **Sfârşit** pentru a termina configurarea.
36. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Da, activare filtre de politică generate**, apoi selectaţi **Permitere totală a celuilalt trafic**.
37. Apăsaţi **OK** pentru a încheia configurarea. Când veţi fi întrebat, specificaţi că doriţi să activaţi regulile pe alte interfeţe.

Operaţii înrudite

"Configurarea VPN pentru Sistem C"
Urmaţi aceeaşi paşi folosiţi pentru a configura VPN pentru Sistem A, cu modificări de adrese IP după caz. Folosiţi ca ghid foile de lucru pentru planificare.

Configurarea VPN pentru Sistem C

Urmaţi aceeaşi paşi folosiţi pentru a configura VPN pentru Sistem A, cu modificări de adrese IP după caz. Folosiţi ca ghid foile de lucru pentru planificare.

După ce terminaţi de configurat gateway-ul VPN al departamentului Finanţe, conexiunile dumneavoastră vor fi într-o stare *la-cerere*, ceea ce înseamnă că pornesc atunci când sunt trimise datagramele IP pe care trebuie să le protejeze această conexiune VPN. Următorul pas este să porniţi serverele VPN, dacă nu sunt deja pornite.

Operaţii înrudite

"Configurarea VPN pentru Sistem A" la pagina 16
Finalizaţi această operaţie pentru a configura Sistem A

Pornire VPN

După ce v-aţi configurat conexiunea VPN pentru Sistem A şi C trebuie să porniţi conexiunea dumneavoastră VPN.

Urmaţi aceşti paşi pentru a porni VPN:

1. În System i Navigator, expandaţi **sistem → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **VPN** şi selectaţi **Pornire**.

Testarea unei conexiuni

După ce aţi terminat de configurat ambele sisteme şi aţi pornit cu succes serverele VPN, testaţi conectivitatea pentru a vă asigura că subreţelele la distanţă pot comunica între ele.

Pentru a vă testa conexiunea, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **Sistem A → Reţea**.
2. Faceţi clic dreapta pe **Configurarea TCP/IP** şi selectaţi **Utilitare** şi apoi selectaţi **Ping**.
3. Din caseta de dialog **Ping de la**, introduceţi Sistem C în câmpul **Ping**.
4. Apăsaţi **Ping acum** pentru a verifica conectivitatea de la Sistem A la Sistem C.
5. Faceţi clic pe **OK** când aţi terminat.

Scenariu: Conexiunea de bază companie la companie

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

Situaţie

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

Se consideră situaţia în care sunteţi un furnizor important de subansamble al unui producător. Pentru că este vital să aveţi produsele specifice şi cantităţile exact la timpul cerut de firma producătoare, trebuie să dispuneţi mereu de starea inventarului producătorului şi de programele de producţie. Poate că în prezent realizaţi această interacţiune manual şi

constataţi că este mare consumatoare de timp, implică un cost ridicat şi uneori apar date eronate. Ca urmare, vreţi să găsiţi o cale mai uşoară, mai rapidă şi mai eficientă pentru comunicarea cu compania producătorului. Având în vedere confidenţialitatea cestor informaţii, producătorul nu doreşte să le publice pe propriul sit Web sau să le distribuie lunar printr-un raport extern. Prin exploatarea Internetului public, puteţi stabili uşor un VPN pentru a îndeplini cererile ambelor companii.

Obiective

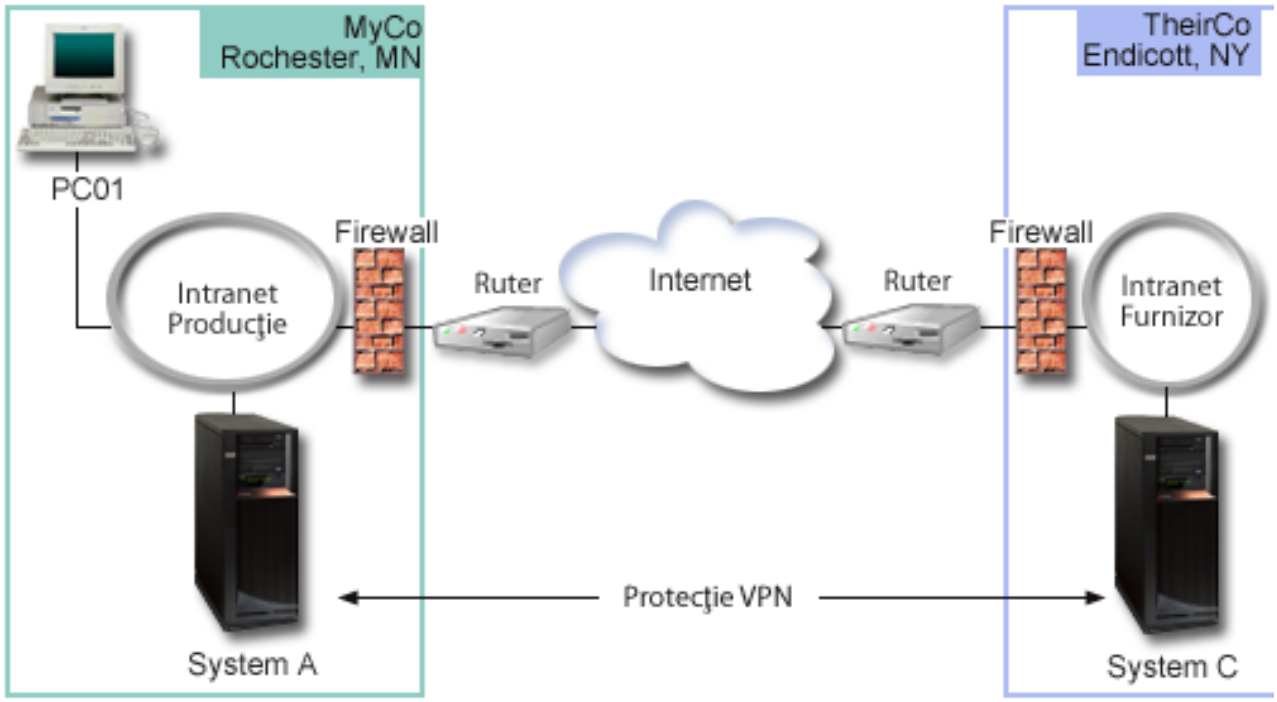
În acest scenariu, MyCo vrea să stabilească un VPN între o gazdă din divizia sa de subansamble şi o gazdă din departamentul de producţie al unuia dintre partenerii de afaceri, TheirCo.

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

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

Detalii

Următoarea ilustraţie prezintă caracteristicile de reţea ale MyCo şi TheirCo:



Reţeaua de aprovizionare MyCo

- Sistem A rulează cu i5/OS Versiunea 5 Ediţia 3 (V5R3), sau mai nou.
- Sistem A are adresa IP 10.6.1.1. Aceasta este punctul final al conexiunii, precum şi punctul final de date. Acesta este, Sistem A realizează negocieri IKE şi aplică IPSec datagramelor IP de intrare şi ieşire şi este de asemenea sursa şi destinaţia datelor care trec prin VPN.
- Sistem A se află în subreţeaua 10.6.0.0 cu masca 255.255.0.0

- Doar Sistem A poate iniţia conexiunea cu Sistem C.

Reţeaua de producţie a TheirCo

- Sistem C rulează cu i5/OS Versiunea 5 Ediţia 3 (V5R3), sau mai nou.
- Sistem C are adresa IP 10.196.8.6. Aceasta este punctul final al conexiunii, precum şi punctul final de date. Acesta este, Sistem A realizează negocieri IKE şi aplică IPSec datagramelor IP de intrare şi ieşire şi este de asemenea sursa şi destinaţia datelor care trec prin VPN.
- Sistem C se află în subreţeaua 10.196.8.0 cu masca 255.255.255.0

Taskurile de configurare

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

Notă: Înainte de a porni aceste operaţii verificaţi rutarea TCP/IP pentru a vă asigura că cele două sisteme gateway pot comunica între ele prin Internet. În acest fel, vă asiguraţi că gazdele din fiecare subreţea rutează corespunzător către gateway-ul corespunzător pentru a accesa subreţeaua la distanţă.

Concepte înrudite

Rutarea TCP/IP şi echilibrarea încărcării

Completarea fişelor de lucru pentru planificare

Lista de verificare de planificare ilustrează tipul de informaţii de care aveţi nevoie înainte de a începe configurarea VPN-ului. Toate răspunsurile din lista de verificare a cerinţei preliminare trebuie să fie Da înainte de a continua cu setarea VPN.

Notă: Aceste fişe de lucru se aplică pentru Sistem A, repetaţi procesul pentru Sistem C, prin inversarea adreselor IP după nevoie.

Tabela 3. Cerinţe sistem

Listă de verificare pentru cerinţele preliminare	**Răspunsuri**
Sistemul rulează i5/OS V5R3, sau mai nou?	Da
Este instalată opţiunea Digital Certificate Manager?	Da
Este instalat System i Access pentru Windows?	Da
Este instalat System i Navigator?	Da
Este instalată subcomponenta Reţea din System i Navigator?	Da
Este instalat IBM TCP/IP Connectivity Utilities for i5/OS?	Da
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe sistem (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH şi ESP?	Da
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	Da

Tabela 4. Configuraţie VPN

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul	**Răspunsuri**
Ce tip de conexiune creaţi ?	gateway-la-gateway
Cum veţi denumi grupul de chei dinamice?	HRgw2FINgw
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja cheile?	echilibrate
Folosiţi 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 ?	Subreţea: 10.6.0.0 Mască: 255.255.0.0
Care este identificatorul serverului de chei la distanţă ?	Adresa IP: 208.222.150.250
Care este identificatorul punctului final de date la distanţă ?	Subreţea: 10.196.8.0 Mască: 255.255.255.0
Ce porturi şi protocoale doriţi să permiteţi prin conexiune ?	Oricare
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja datele?	echilibrate
Pe care dintre interfeţe se aplică această conexiune ?	TRLINE

Configurarea VPN pentru Sistem A

Finalizaţi următorii paşi pentru a configura o conexiune VPN pentru Sistem A.

Folosiţi informaţiile din fişele de lucru pentru planificare pentru a configura VPN pentru Sistem A după cum urmează:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi MyCo2TheirCo.
6. Opţional: Specificaţi o descriere pentru acest grup de conexiuni.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gazdei dumneavoastră la altă gazdă**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Crearea unei noi politici** şi apoi selectaţi **Cea mai înaltă securitate, cea mai joasă performanţă**.
11. Apăsaţi pe **Următor** pentru a merge la pagina **Certificat pentru punct final al conexiunii locale**.
12. Selectaţi **Da** pentru a indica dacă veţi folosi certificate pentru autentificarea conexiunii. Apoi, selectaţi certificatul care reprezintă Sistem A.

    Notă: Dacă vreţi să folosiţi un certificat pentru autentificarea punctului final al conexiunii locale, trebuie să creaţi întâi certificatul în DCM.
13. Apăsaţi **Următor** pentru a merge în pagina **Identificator de punct final al conexiunii locale** .
14. Selectaţi **Adresa IP Versiunea 4** ca tip de identificator. Adresa IP asociată trebuie să fie 10.6.1.1. Din nou, aceste informaţii sunt definite în certificatul pe care îl creaţi în DCM.
15. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
16. Selectaţi **Adresa IP Versiunea 4** din câmpul **Tip de identificator**.
17. Introduceţi 10.196.8.6 în câmpul **Identificator**.
18. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
19. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge în pagina **Politică de date**.

20. Selectaţi **Crearea unei noi politici** şi apoi selectaţi **Cea mai înaltă securitate, cea mai joasă performanţă**. Selectaţi **Folosirea algoritmului de criptare RC4**.
21. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
22. Selectaţi **TRLINE**.
23. Apăsaţi **Următor** pentru a merge la pagina **Sumar**. Revedeţi obiectele pe care le va crea pentru a asigura corectitudinea lor.
24. Apăsaţi pe **Sfârşit** pentru a termina configurarea.
25. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Nu, regulile pachet vor fi activate la un moment ulterior** apoi faceţi clic pe **Ok**.

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

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

Configurarea VPN pentru Sistem C

Urmaţi aceeaşi paşi folosiţi pentru a configura VPN pentru Sistem A, cu modificări de adrese IP după caz. Folosiţi ca ghid foile de lucru pentru planificare.

După ce terminaţi de configurat gateway-ul VPN al departamentului Finanţe, conexiunile dumneavoastră vor fi într-o stare *la-cerere*, ceea ce înseamnă că pornesc atunci când sunt trimise datagramele IP pe care trebuie să le protejeze această conexiune VPN. Următorul pas este să porniţi serverele VPN, dacă nu sunt deja pornite.

Activare reguli pachet

Vrăjitorul pentru VPN creează regulile pachet de care această conexiune are nevoie pentru a funcţiona corect. Oricum, trebuie să le activaţi pe ambele sisteme înainte de a porni conexiunea VPN.

Pentru a activa regulile pachet pe Sistem A, urmaţi aceşti paşi:

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

Pornirea unei conexiuni

După ce v-aţi configurat conexiunea VPN trebuie să vă porniţi conexiunea VPN.

Urmaţi aceşti paşi pentru a porni conexiunea MyCo2TheirCo de pe Sistem A:

1. În System i Navigator, expandaţi **Sistem A → Reţea → Politici IP**.
2. Dacă serverul VPN nu este pornit, faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Pornire**. Aceasta porneşte serverul VPN.
3. Expandaţi **VPN → Conexiuni securizate**.

4. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
5. Faceţi clic dreapta pe **MyCo2TheirCo** şi selectaţi **Pornire**.
6. Din meniul **Vizualizare**, selectaţi **Reîmprospătare**. Dacă conexiunea porneşte cu succes, starea se va modifica din *Inactivă* în *Activată*. Conexiunea s-ar putea să aibă nevoie de câteva minute pentru a porni, astfel reîmprospătaţi în mod periodic până când starea se modifică la *Activat*.

Testarea unei conexiuni

După ce aţi terminat de configurat ambele sisteme şi aţi pornit cu succes serverele VPN, testaţi conectivitatea pentru a vă asigura că subreţelele la distanţă pot comunica între ele.

Pentru a vă testa conexiunea, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **Sistem A → Reţea**.
2. Faceţi clic dreapta pe **Configurarea TCP/IP** şi selectaţi **Utilitare** şi apoi selectaţi **Ping**.
3. Din caseta de dialog **Ping de la**, introduceţi Sistem C în câmpul **Ping**.
4. Apăsaţi **Ping acum** pentru a verifica conectivitatea de la Sistem A la Sistem C.
5. Faceţi clic pe **OK** când aţi terminat.

Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec

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

Situaţie

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

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

Important: Acest scenariu arată gateway-urile de securitate ataşate direct la Internet. Absenţa unui firewall are intenţia de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile de securitate implicate de fiecare dată când vă conectaţi la Internet.

Obiective

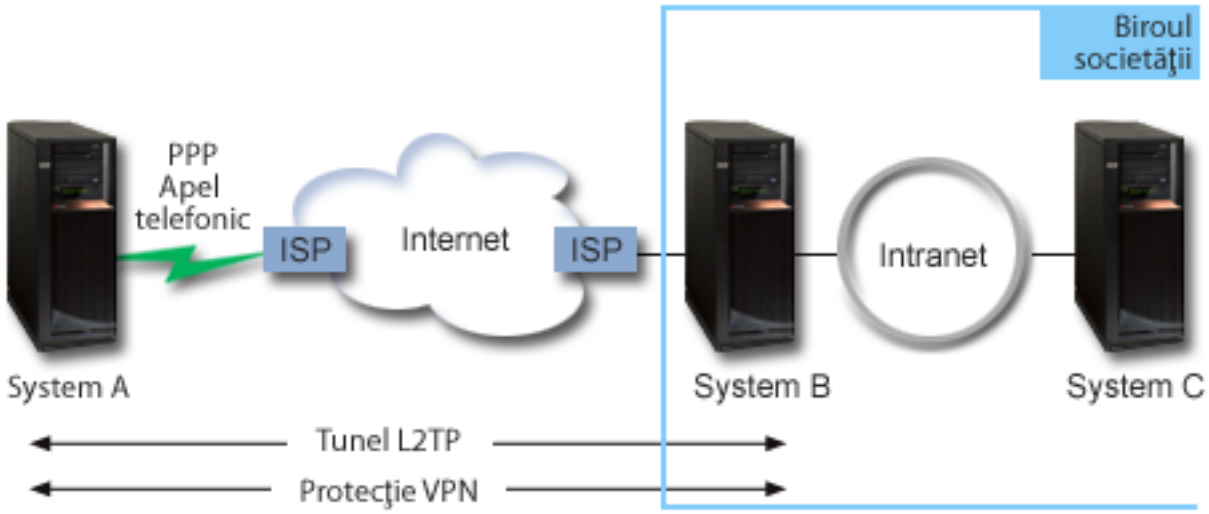
În acest scenariu, un sistem al filialei se conectează la reţeaua companiei printr-un sistem gateway cu un tunel L2TP protejat de VPN.

Obiectivele principale ale acestui scenariu sunt:

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

Detalii

Următoarea ilustraţi prezintă caracteristicile reţelei pentru acest scenariu:



Sistem A

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

Sistem B

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

În termeni L2TP, *Sistem A* are rol de iniţiator L2TP, în timp ce *Sistem B* are rol de terminator L2TP.

Taskurile de configurare

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

Concepte înrudite

“Layer 2 Tunnel Protocol” la pagina 7
Conexiunile L2TP (Layer 2 Tunneling Protocol), care mai sunt numite linii virtuale, furnizează acces eficient utilizatorilor la distanţă prin permiterea unei reţele de sisteme comune să gestioneze adresele IP asignate utilizatorilor la distanţă. Mai mult, conexiunile L2TP furnizează acces sigur la sistemul sau reţeaua dumneavoastră când le folosiţi împreună cu IP Security (IPSec).

Informaţii înrudite

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

Configurarea VPN pentru Sistem A

Finalizaţi următorii paşi pentru a configura o conexiune VPN pentru Sistem A.

Folosiţi informaţiile din fişele de lucru pentru planificare pentru a configura VPN pentru Sistem A după cum urmează:

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

      Notă: Dacă folosiţi chei prepartajate şi negociere în modul agresiv în configuraţia dumneavoastră, selectaţi pentru parole cuvinte necunoscute, pentru care este mică probabilitatea de a fi sparte în atacurile care scanează un dicţionar. Se recomandă de asemenea să vă modificaţi periodic parolele.
   k. Apăsaţi **OK** pentru a salva configuraţia.
2. **Configurare politică de date**
   a. Din interfaţa VPN, faceţi clic dreapta pe **Politici de date** şi selectaţi **Politică nouă de date**.
   b. În pagina **General**, specificaţi numele politicii de date. De exemplu, l2tpremoteuser.
   c. Mergeţi la pagina **Propuneri**. O propunere este o colecţie de protocoale pe care le folosesc serverele de chei iniţiatoare şi respondente pentru a stabili o conexiune dinamică între două capete. Puteţi folosi o singură politică de date în mai multe obiecte conexiune. Însă nu toate serverele de chei VPN la distanţă trebuie neapărat să aibă aceleaşi proprietăţi pentru politica de date. De aceea, puteţi adăuga mai multe propuneri pentru aceeaşi politică de date. La stabilirea unei conexiuni cu un server la distanţă, trebuie să fie cel puţin o propunere corespunzătoare în politica de date a iniţiatorului şi respondentului.
   d. Apăsaţi **Adăugare** pentru a adăuga o transformare de politică de date.
   e. Selectaţi **Transport** pentru modul de încapsulare.
   f. Apăsaţi **OK** pentru a reveni la pagina **Transformări**.
   g. Specificaţi o valoare pentru expirarea cheii.
   h. Apăsaţi **OK** pentru a salva noua politică de date.
3. **Configurarea grupului de chei dinamice**
   a. Din interfaţa VPN, expandaţi **Conexiuni securizate**.
   b. Faceţi clic dreapta pe **După grup** şi selectaţi **Grup nou de chei dinamice**.
   c. În pagina **General**, specificaţi un nume pentru grup. De exemplu, l2tptocorp.
   d. Selectaţi **Protejare tunel L2TP iniţiat local**.

e. Pentru rolul sistemului, selectaţi **Ambele sisteme sunt gazde**.

f. Mergeţi la pagina **Politică**. Selectaţi politica de date pe care aţi creat-o la pasul **Configurarea politicii de date**, l2tpremoteuser, din lista **Politică de date**.

g. Selectaţi **Sistem local iniţiază conexiune** pentru a indica faptul că doar Sistem A poate iniţia conexiuni cu Sistem B.

h. Mergeţi la pagina **Conexiuni**. Selectaţi **Generare următoarea regulă de filtrare politici pentru acest grup**. Apăsaţi **Editare** pentru a defini parametrii filtrului de politici.

i. În pagina **Filtru de politică - Adrese locale**, selectaţi **Identificator cheie** drept tipul identificatorului.

j. Pentru identificator, selectaţi identificatorul de cheie, thisisthekeyid, pe care l-aţi definit în politica IKE.

k. Mergeţi la pagina **Filtru politică - Adrese la distanţă**. Selectaţi **Adresă IP Versiunea 4** din lista **Tip identificator**.

l. Introduceţi 205.13.237.6 în câmpul **Identificator**.

m. Mergeţi la pagina **Filtru politică - Servicii**. Introduceţi 1701 în câmpurile **Port local** şi **Port la distanţă**. Portul 1701 este binecunoscutul port pentru L2TP.

n. Selectaţi **UDP** din lista **Protocol**.

o. Apăsaţi **OK** pentru a reveni la pagina **Conexiuni**.

p. Mergeţi la pagina **Interfeţe**. Selectaţi orice profil linie sau PPP pentru care se va aplica acest grup. Încă nu aţi creat profilul PPP pentru acest grup. După ce faceţi acest lucru, va trebui să editaţi proprietăţile acestui grup astfel încât grupul să se aplice pentru profilul PPP pe care îl creaţi în pasul următor.

q. Apăsaţi **OK** pentru a crea grupul de chei dinamice, l2tptocorp.

4. **Configurarea conexiunii cu chei dinamice**

a. Din interfaţa VPN, expandaţi **După grup**. Astfel se afişează o listă cu toate grupurile de chei dinamice configurate pe Sistem A.

b. Faceţi clic dreapta pe **l2tptocorp** şi selectaţi **Conexiune nouă cu chei dinamice**.

c. În pagina **General**, specificaţi o descriere opţională a conexiunii.

d. Pentru serverul de chei la distanţă, selectaţi **Adresă IP v4** pentru tipul identificatorului.

e. Selectaţi 205.13.237.6 din lista **Adresa IP**.

f. Deselectaţi **Pornire la-cerere**.

g. Mergeţi la pagina **Adrese locale**. Selectaţi **Identificator cheie** pentru tipul identificatorului şi apoi selectaţi thisisthekeyid din lista **Identificator**.

h. Mergeţi la pagina **Adrese la distanţă**. Selectaţi **Adresă IP Versiunea 4** pentru tipul identificatorului.

i. Introduceţi 205.13.237.6 în câmpul **Identificator**.

j. Mergeţi la pagina **Servicii**. Introduceţi 1701 în câmpurile **Port local** şi **Port la distanţă**. Portul 1701 este binecunoscutul port pentru L2TP.

k. Selectaţi **UDP** din lista **Protocol**.

l. Apăsaţi **OK** pentru a crea conexiunea cu cheie dinamică.

Operaţii înrudite

"Configurarea VPN pentru Sistem B" la pagina 27
Pentru a configura o conexiune VPN pentru Sistem B urmaţi aceeaşi paşi de la configurarea unei conexiuni pentru Sistem A şi modificaţi adrese IP şi identificatori după caz.

Configurarea unui profil de conexiune PPP şi linie virtuală pe Sistem A

Acum că pe Sistem A este configurată o conexiune VPN trebuie să creaţi profilul PPP pentru Sistem A. Profilul PPP nu are o linie fizică asociată acestuia; în schimb, foloseşte o linie virtuală. Aceasta deoarece traficul PPP trece prin tunelul L2TP, în timp ce VPN protejează tunelul L2TP.

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

1. În System i Navigator, expandaţi **Sistem A → Reţea → Serviciide acces la distanţă**.
2. Faceţi clic dreapta pe **Profiluri de conexiune iniţiator** şi selectaţi **Profil nou**.

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

Aplicarea grupului de chei dinamice l2tptocorp la profilul PPP toCorp

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

Pentru a asocia grupul dumneavoastră de chei dinamice cu profilul dumneavoastră PPP urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate → După grup**.
2. Faceţi clic dreapta pe grupul de chei dinamice, l2tptocorp, şi selectaţi **Proprietăţi**.

3. Mergeţi la pagina **Interfeţe** şi selectaţi **Aplicare acest grup** pentru profilul PPP pe care l-aţi creat în pasul “Configurarea unui profil de conexiune PPP şi linie virtuală pe Sistem A” la pagina 25, toCorp.
4. Apăsaţi **OK** pentru a aplica l2tptocorp la profilul PPP, toCorp.

Configurarea VPN pentru Sistem B

Pentru a configura o conexiune VPN pentru Sistem B urmaţi aceeaşi paşi de la configurarea unei conexiuni pentru Sistem A şi modificaţi adrese IP şi identificatori după caz.

Luaţi în calcul şi aceste puncte înainte să începeţi:

- Identificare server de chei la distanţă după identificator cheie pe care l-aţi specificat pentru serverul de chei local pentru Sistem A. De exemplu thisisthekeyid.
- Folosiţi *exact* aceeaşi cheie prepartajată.
- Asiguraţi-vă că transformările dumneavoastră se potrivesc cu cele configurate pe Sistem A, altfel conexiunile vor eşua.
- Nu specificaţi **Protejare tunel L2TP iniţiat local** pe pagina **General** a grupului de chei dinamice.
- Sistemul la distanţă iniţiază conexiunea.
- Specificaţi pornirea la cerere a conexiunii.

Operaţii înrudite

“Configurarea VPN pentru Sistem A” la pagina 24
Finalizaţi următorii paşi pentru a configura o conexiune VPN pentru Sistem A.

Configurarea unui profil de conexiune PPP şi linie virtuală pe Sistem B

Acum că pe Sistem A este configurată o conexiune VPN trebuie să creaţi profilul PPP pentru Sistem B. Profilul PPP nu are o linie fizică asociată acestuia; în schimb, foloseşte o linie virtuală. Aceasta deoarece traficul PPP trece prin tunelul L2TP, în timp ce VPN protejează tunelul L2TP.

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

1. În System i Navigator, expandaţi **Sistem A → Reţea → Serviciide acces la distanţă**.
2. Faceţi clic dreapta pe **Profiluri de conexiune respondent** şi selectaţi **Profil nou**.
3. În pagina **Setare**, selectaţi **PPP** pentru tipul protocolului.
4. Pentru Selecţii mod, selectaţi **L2TP (linie virtuală)**.
5. Selectaţi **Terminator (server de reţea)** din lista **Modul de operare**.
6. Apăsaţi **OK** pentru pagina Proprietăţi profiluri PPP.
7. În pagina **General**, introduceţi un nume care identifică tipul şi destinaţia conexiunii. În acest caz, introduceţi tobranch. Numele trebuie pe care îl specificaţi trebuie să fie de 10 caractere sau mai puţin.
8. Opţional: Specificaţi o descriere pentru profil
9. Mergeţi la pagina **Conexiune**.
10. Selectaţi adresa IP a punctului final local al tunelului, 205.13.237.6.
11. În câmpul **Nume linie virtuală**, selectaţi **tobranch** din lista derulantă. Ţineţi minte că această linie nu are interfeţe fizice asociate. Linia virtuală descrie diferite caracteristici ale acestui profil PPP; de exemplu, dimensiunea maximă a cadrului, informaţii despre autentificare, nume gazdă local etc. Apare caseta de dialog **Proprietăţi linie L2TP**.
12. În pagina **General**, introduceţi o descriere pentru linia virtuală.
13. Mergeţi la pagina **Autentificare**.
14. În câmpul **Nume gazdă local**, introduceţi numele gazdă al serverului de chei local, Sistem A.
15. Apăsaţi **OK** pentru a salva descrierea liniei virtuale noi şi reveniţi la pagina **Conexiune**.
16. Mergeţi la pagina **Setări TCP/IP**.
17. În secţiunea **Adresă IP locală**, selectaţi adresa IP fixă a sistemului local, 10.6.11.1.

18. În secţiunea **Adresă IP la distanţă**, selectaţi **Pool de adrese** ca metodă de atribuire a adresei. Introduceţi o adresă de pornire şi apoi specificaţi numărul de adrese care pot să fie atribuite sistemului la distanţă.
19. Selectaţi **Permitere sistemului de la distanţă să acceseze alte reţele (înaintare IP)**.
20. Mergeţi la pagina **Autentificare** pentru a seta numele utilizatorului şi parola pentru acest profil PPP.
21. În secţiunea Identificare sistem local, selectaţi **Permitere sistemului de la distanţă să verifice identitatea acestui sistem**. Aceasta deschide caseta de dialog **Identificare sistem local**.
22. Sub **Protocol de autentificare de folosit** selectaţi **Este necesară parolă criptată (CHAP-MD5)**.
23. Introduceţi numele utilizatorului, Sistem A, şi o parolă.
24. Apăsaţi **OK** pentru a salva profilul PPP.

Activare reguli pachet

Vrăjitorul pentru VPN creează regulile pachet de care această conexiune are nevoie pentru a funcţiona corect. Oricum, trebuie să le activaţi pe ambele sisteme înainte de a porni conexiunea VPN.

Pentru a activa regulile pachet pe Sistem A, urmaţi aceşti paşi:

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

Scenariu: VPN prietenos pentru firewall-uri

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

Situaţie

Presupunem că sunteţi o mare companie de asigurări pentru locuinţe cu sediul în Minneapolis şi aţi deschis de curând o filială la Chicago. Filiala din Chicago are nevoie să acceseze baza de date a clienţilor care se află la sediul central din Minneapolis. Vreţi să fiţi sigur că informaţiile transferate sunt securizate, deoarece baza de date conţine date confidenţiale despre clienţii dumneavoastră, cum ar fi: numele, adresele şi numerele de telefon. Vă decideţi să conectaţi ambele filiale prin internet prin utilizarea unui VPN (virtual private network). Ambele filiale se află în spatele unui firewall şi folosesc NAT (network address translation) pentru a îşi ascunde adresele IP private neînregistrate în spatele unui set de adrese IP înregistrate. Dar, conexiunile VPN au câteva incompatibilităţi 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. Totuşi, puteţi folosi o conexiune VPN cu NAT dacă implementaţi încapsularea UDP.

În acest scenariu, adresa IP privată a reţelei Chicago este pusă într-un nou antet şi este translatată când trece prin Firewall C (vedeţi imagina următoare). Apoi, când pachetul ajunge la Firewall D, acesta va translata adresa IP destinaţie la adresa IP a Sistem E, prin urmare pachetul va fi înaintat la Sistem E. În cele din urmă, când pachetul ajunge la Sistem E acesta renunţă la antetul UDP, ceea ce rămâne este pachetul IPSec original, care acum va trece de toate validările şi va permite o conexiune VPN securizată.

Obiective

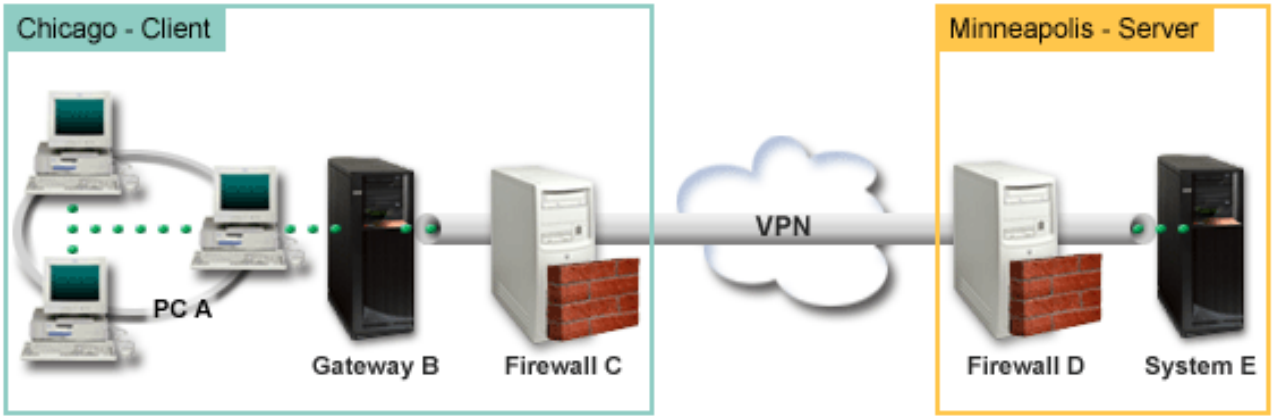
În acest scenariu, o companie de asigurări mare vrea să stabilească un VPN între un gateway din Chicago (client) şi o gazdă din Minneapolis (server), atunci când amândouă reţelele sunt în spatele unui firewall.

Obiectivele acestui scenariu sunt următoarele:

- Gateway-ul filialei din Chicago iniţiază întotdeauna conexiunea la gazda din Minneapolis.
- VPN trebuie să protejeze tot traficul de date între gateway-ul din Chicago şi gazda din Minneapolis.
- Se permite tuturor utilizatorilor din gateway-ul din Chicago să acceseze o bază de date System i care se află în reţeaua din Minneapolis printr-o conexiune VPN.

Detalii

Următoarea ilustraţi prezintă caracteristicile reţelei pentru acest scenariu:



Reţeaua Chicago - Client

- Gateway B rulează cu i5/OS Versiunea 5 Ediţia 4 (V5R4), sau mai nou.
- Gateway B se conectează la internet cu adresa IP 214.72.189.35 şi este punctul final al conexiunii al tunelului VPN. Gateway B realizează negocieri IKE şi aplică încapsulări UDP datagramelor IP de ieşire.
- Gateway B şi PC A sunt în subreţeaua 10.8.11.0 cu masca 255.255.255.0
- PC A este sursa şi destinaţia pentru datele care trec prin conexiunea VPN, prin urmare este punctul final al tunelului VPN.
- Doar Gateway B poate iniţia conexiunea cu Sistem E.
- Firewall C are o regulă Masq NAT cu adresa IP publică 129.42.105.17 care ascunde adresa IP de la Gateway B

Reţeaua Minneapolis - Server

- Sistem E rulează cu i5/OS Versiunea 5 Ediţia 4 (V5R4), sau mai nou.
- Sistem E are adresa IP 56.172.1.1.
- Sistem E este respondentul în acest scenariu.
- Firewall D are adresa IP 146.210.18.51.
- Firewall D are o regulă Static NAT care mapează IP-ul public (146.210.18.15) la IP-ul privat de la Sistem E (56.172.1.1). Prin urmare, din perspectiva clientului adresa IP pentru Sistem E este adresa IP publică (146.210.18.51) de la Firewall D.

Taskurile de configurare

Concepte înrudite

“Gestionarea cheilor” la pagina 6
Un VPN dinamic furnizează securitate suplimentară pentru comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.

“IPSec compatibil NAT cu UDP” la pagina 9
Încapsularea UDP permite traficului IPSec să treacă printr-un dispozitiv NAT convenţional. Treceţi în revistă acest subiect pentru mai multe informaţii despre ce este şi de ce ar trebui să îl folosiţi pentru conexiunile dumneavoastră VPN.

Completarea fişelor de lucru de planificare

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

Notă: Există fişe de lucru separate atât pentru Gateway B cât şi pentru Sistem E.

Tabela 5. Cerinţe sistem

Listă de verificare pentru cerinţele preliminare	**Răspunsuri**
Sistemul dumneavoastră de operare este i5/OS V5R4, sau mai nou?	Da
Este instalată opţiunea Digital Certificate Manager?	Da
Este instalat System i Access pentru Windows?	Da
Este instalat System i Navigator?	Da
Este instalată subcomponenta Reţea din System i Navigator?	Da
Este instalat IBM TCP/IP Connectivity Utilities for i5/OS?	Da
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe sistem (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite 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. Configuraţie Gateway B

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul pentru Gateway B	**Răspunsuri**
Ce tip de conexiune creaţi ?	gateway-la-altă gazdă
Cum veţi denumi grupul de chei dinamice?	CHIgw2MINhost
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja cheile?	echilibrate
Folosiţi certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată?	Nu : topsecretstuff
Care este identificatorul serverului de chei local?	Adresa IP: 214.72.189.35
Care este identificatorul punctului final de date local ?	Subreţea: 10.8.11.0 Mască: 255.255.255.0
Care este identificatorul serverului de chei la distanţă ?	Adresa IP: 146.210.18.51
Care este identificatorul punctului final de date la distanţă ?	Adresa IP: 146.210.18.51

Tabela 6. Configuraţie Gateway B (continuare)

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul pentru Gateway B	**Răspunsuri**
Ce porturi şi protocoale doriţi să permiteţi prin conexiune ?	Oricare
De ce tip de securitate şi performanţă sistem aveţi nevoie pentru a vă proteja datele?	echilibrate
Pe care dintre interfeţe se aplică această conexiune ?	TRLINE

Tabela 7. Configuraţie Sistem E

Aveţi nevoie de aceste informaţii pentru a configura VPN-ul pentru Sistem E	**Răspunsuri**
Ce tip de conexiune creaţi ?	gazdă-la-alt gateway
Cum veţi denumi grupul de chei dinamice?	CHIgw2MINhost
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile?	cele mai înalte
Folosiţi certificate pentru autentificarea conexiunii? Dacă nu, care este cheia prepartajată?	Nu : topsecretstuff
Care este identificatorul serverului de chei local?	Adresa IP: 56.172.1.1
Care este identificatorul serverului de chei la distanţă? **Notă:** Dacă adresa IP Firewall C nu se cunoaşte, puteţi folosi *ANYIP ca identificator pentru serverul de chei la distanţă.	Adresa IP: 129.42.105.17
Care este identificatorul punctului final de date la distanţă ?	Subreţea: 10.8.11.0 Mască: 255.255.255.0
Ce porturi şi protocoale doriţi să permiteţi prin conexiune ?	Oricare
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja datele?	cele mai înalte
Pe care dintre interfeţe se aplică această conexiune ?	TRLINE

Referinţe înrudite

Consilier planificare VPN

Configurarea VPN pentru Gateway B

Finalizaţi următorii paşi pentru a configura o conexiune VPN pentru Gateway B.

Folosiţi informaţiile din fişele de lucru de planificare pentru a configura VPN pentru Gateway B după cum urmează:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi CHIgw2MINhost.
6. Opţional: Specificaţi o descriere pentru acest grup de conexiuni.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gateway-ului dumneavoastră la altă gazdă**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.

    Notă: Dacă primiţi un mesaj de eroare care spune ″Cererea de certificat nu a putut fi procesată″ puteţi să-l ignoraţi, deoarece nu folosiţi certificate pentru schimbul de chei.
11. Opţional: Dacă aveţi certificate instalate veţi vedea pagina **Certificat pentru punctul final al conexiunii locale**. Selectaţi Nu pentru a indica că nu veţi folosi certificate pentru a autentifica conexiunea.
12. Apăsaţi **Următor** pentru a merge la pagina **Server de chei local**.
13. Selectaţi **IP versiunea 4** din câmpul **Tip identificator**.
14. Selectaţi 214.72.189.35 din câmpul **Adresă IP**.

15. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
16. Selectaţi **Adresă IP versiunea 4** în câmpul **Tip identificator**.
17. Introduceţi 146.210.18.51 în câmpul **Identificator**.

    Notă: Dacă gateway-ul B iniţiază o conexiune la un Static NAT trebuie să specificaţi modul principal de schimbare de chei pentru a introduce o singură adresă IP pentru cheia de la distanţă. Modul principal de schimb de chei este selectat implicit când creaţi o conexiune cu vrăjitorul de conexiuni VPN. Dacă este folosit modul agresiv în această situaţie, trebuie introdus pentru cheia de la distanţă un tip de identificator la distanţă diferit de IPV4.
18. Introduceţi topsecretstuff în câmpul **Cheie prepartajată**.
19. Apăsaţi **Următor** pentru a merge la pagina **Punct final local de date**.
20. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
21. Introduceţi 10.8.0.0 în câmpul **Identificator**.
22. Introduceţi 255.255.255.0 în câmpul **Mască subreţea**.
23. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
24. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge la pagina Politică de date.
25. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.
26. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
27. Selectaţi **TRLINE** din tabelul Linie.
28. Apăsaţi **Următor** pentru a merge la pagina **Sumar**.
29. Revedeţi obiectele pe care le va crea pentru a asigura corectitudinea lor.
30. Apăsaţi pe **Sfârşit** pentru a termina configurarea.
31. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Da**, activare filtre de politică generate, apoi selectaţi **Permitere totală a celuilalt trafic**.
32. Apăsaţi **OK** pentru a încheia configurarea.

Configurarea VPN pentru Sistem E

Finalizaţi următorii paşi pentru a configura o conexiune VPN pentru Sistem E.

Folosiţi informaţiile din fişele dumneavoastră de lucru pentru planificare pentru a configura VPN pentru Sistem E după cum urmează:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul Conexiune.
3. Revedeţi pagina **Bine aţi venit** pentru informaţii despre ce obiecte creează vrăjitorul.
4. Faceţi clic pe **Următor** pentru a merge la pagina **Nume conexiune**.
5. În câmpul **Nume**, introduceţi CHIgw2MINhost.
6. Opţional: Specificaţi o descriere pentru acest grup de conexiuni.
7. Faceţi clic pe **Următor** pentru a merge la pagina **Scenariu conexiune**.
8. Selectaţi **Conectarea gazdei dumneavoastră la alt gateway**.
9. Faceţi clic pe **Următor** pentru a merge la pagina **Politica Internet Key Exchange**.
10. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.

    Notă: Dacă primiţi un mesaj de eroare care spune ″Cererea de certificat nu a putut fi procesată″ puteţi să-l ignoraţi, deoarece nu folosiţi certificate pentru schimbul de chei.
11. Opţional: Dacă aveţi certificate instalate veţi vedea pagina **Certificat pentru punctul final al conexiunii locale**. Selectaţi Nu pentru a indica că nu veţi folosi certificate pentru a autentifica conexiunea.
12. Apăsaţi **Următor** pentru a merge la pagina **Server de chei local**.
13. Selectaţi **Adresă IP versiunea 4** în câmpul **Tip identificator**.

14. Selectaţi 56.172.1.1 din câmpul **Adresă IP**.
15. Apăsaţi **Următor** pentru a merge la pagina **Server de chei la distanţă**.
16. Selectaţi **Adresă IP versiunea 4** în câmpul **Tip identificator**.
17. Introduceţi 129.42.105.17 în câmpul **Identificator**.

    Notă: Dacă adresa IP Firewall C nu se cunoaşte, puteţi folosi *ANYIP ca identificator pentru serverul de chei la distanţă.
18. Introduceţi topsecretstuff în câmpul **Cheie prepartajată**.
19. Apăsaţi **Următor** pentru a merge la pagina **Punct final de date distanţă**.
20. Selectaţi **Subreţea IP versiunea 4** din câmpul **Tip identificator**.
21. Introduceţi 10.8.11.0 în câmpul **Identificator**.
22. Introduceţi 255.255.255.0 în câmpul **Mască subreţea**.
23. Apăsaţi **Următor** pentru a merge în pagina **Servicii de date**.
24. Acceptaţi valorile implicite şi apoi apăsaţi **Următor** pentru a merge la pagina Politică de date.
25. Selectaţi **Creare politică nouă** şi apoi selectaţi **Echilibrare securitate şi performanţă**.
26. Apăsaţi **Următor** pentru a merge la pagina **Interfeţe aplicabile**.
27. Selectaţi **TRLINE** din tabelul Linie.
28. Apăsaţi **Următor** pentru a merge la pagina **Sumar**.
29. Revedeţi obiectele pe care le va crea pentru a asigura corectitudinea lor.
30. Apăsaţi pe **Sfârşit** pentru a termina configurarea.
31. Când apare caseta de dialog **Activare filtre politică**, selectaţi **Da**, activare filtre de politică generate, apoi selectaţi **Permitere totală a celuilalt trafic**.
32. Apăsaţi **OK** pentru a încheia configurarea.

Pornire Conexiune

După ce v-aţi configurat conexiunea VPN pentru Sistem E trebuie să vă porniţi conexiunea VPN.

Urmaţi aceşti paşi pentru a confirma că CHIgw2MINhost este o conexiune activă pentru Sistem E:

1. În System i Navigator, expandaţi **Sistem E → Reţea → Conexiuni securizate → Toate conexiunile**.
2. Vizualizaţi **CHIgw2MINhost** şi verificaţi că **Stare** este *Idle* sau *On-Demand*.

Urmaţi aceşti paşi pentru a porni conexiunea CHIgw2MINhost de la Gateway B:

1. În System i Navigator, expandaţi **Gateway B → Reţea → Politici IP**.
2. Dacă serverul VPN nu este pornit, faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Pornire**.
3. Expandaţi **VPN → Conexiuni securizate**.
4. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
5. Faceţi clic dreapta pe **CHIgw2MINhost** şi selectaţi **Pornire**.
6. Din meniul **Vizualizare**, selectaţi **Reîmprospătare**. Dacă conexiunea porneşte cu succes, **Starea** se va modifica din *Pornire* sau *La cerere* în *Activată*. Conexiunea ar putea avea nevoie de un scurt timp pentru a porni, de aceea trebuie să reîmprospătaţi în mod periodic până când starea se modifică la *Activat*.

Testarea conexiunii

După ce aţi terminat de configurat atât Gateway B cât şi Sistem E şi aţi pornit cu succes serverele VPN, testaţi conectivitatea pentru a vă asigura că ambele sisteme pot comunica între ele.

Pentru a vă testa conexiunile, urmaţi aceşti paşi:

1. Găsiţi un sistem în reţeaua de PC-uri A şi deschideţi o sesiune Telnet.
2. Specificaţi adresa IP publică pentru Sistem E, care este 146.210.18.51.

3. Specificaţi orice informaţie de logare, dacă este necesară. Dacă puteţi vedea ecranul de logare atunci conexiunea funcţionează.

Scenariu: conexiune VPN la utilizatori la distanţă

Administratorul trebuie să configureze o conexiune VPN (virtual private network) la utilizatori la distanţă pentru a activa conexiunile la distanţă.

Următoarele operaţii vă arată cum configurează administratorul o conexiune VPN la utilizatori la distanţă.

Completarea fişelor de lucru pentru planificare pentru conexiune VPN de la filială la comercianţi la distanţă

Administratorul filialei de vânzări foloseşte consilierul de planificare VPN pentru a crea fişe de lucru pentru planificare dinamice pentru a îi ajuta la configurarea VPN (virtual private network) pe sistemele şi staţiile lor de lucru de la distanţă.

Consilierul de planificare VPN este o unealtă interactivă care pune întrebări specifice cu privire la nevoile dumneavoastră VPN. Pe baza răspunsurilor dumneavoastră, consilierul generează o fişă de lucru pentru planificare personalizată pentru mediul dumneavoastră care poate fi folosită la configurarea conexiunii VPN. Această fişă de lucru poate fi folosită la configurarea uni VPN pe sistemul dumneavoastră. Fiecare din următoarele fişe de lucru pentru planificare este generată cu consilierul de planificare VPN şi este folosită pentru a configura un VPN, prin folosirea vrăjitorului VPN Conexiune nouă din System i Navigator.

Tabela 8. Fişă de lucru pentru planificare pentru conexiune VPN între filiala de vânzări şi comercianţi la distanţă

Ce întrebări pune vrăjitorul VPN	**Ce recomandă consilierul VPN**
Cum doriţi să denumiţi acest grup conexiune?	SalestoRemote
Ce tip de grup conexiune aţi dori să creaţi?	Selectaţi **Conectaţi gazda dvs. la altă gazdă**
Ce politică IKE (Internet Key Exchange) doriţi să folosiţi pentru a vă proteja cheile?	Selectaţi **Creare politică nouă** şi apoi selectaţi **cea mai înaltă securitate, cea mai joasă performanţă**
Folosiţi certificate?	Selectaţi **Nu**
Introduceţi identificatorul pentru a reprezenta serverul local de chei pentru această conexiune.	Tip identificator: **adresă IP versiunea 4**, adresa IP:**192.168.1.2**. Pentru adresă IPv6, tip identificator: **adresă IP versiunea 6**, adresa IP:**2001:DB8::2** **Notă:** Adresele IP folosite în acest scenariu sunt folosite doar ca exemplu. Ele nu reflectă o schemă de adrese IP şi nu ar trebui folosite în nici o configuraţie reală. Trebuie să folosiţi propriile dumneavoastră adrese IP când completaţi aceste operaţii.

Tabela 8. Fişă de lucru pentru planificare pentru conexiune VPN între filiala de vânzări şi comercianţi la distanţă (continuare)

Ce întrebări pune vrăjitorul VPN	Ce recomandă consilierul VPN
Care este identificatorul serverului de chei la care doriţi să vă conectaţi?	Tip identificator: **Orice adresă IP**, **Cheie pre-partajată**: mycokey. **Notă:** Cheia pre-partajată este un şir text de 32 de caractere pe care VPN-ul i5/OS îl foloseşte pentru a autentifica conexiune cât şi pentru a stabili cheile care vă protejează datele. În general, ar trebui să trataţi o cheie pre-partajată în acelaşi fel în care trataţi o parolă.
Care sunt porturile şi protocoalele datelor pe care această conexiune le va proteja?	**Port local**: 1701, **Port la distanţă**: orice port, **Protocol**: UDP
Ce politică de date doriţi să folosiţi pentru a proteja datele?	Selectaţi **Creare politică nouă** şi apoi selectaţi **cea mai înaltă securitate, cea mai joasă performanţă**
Bifaţi interfeţele din sistemul local la care va fi aplicată această conexiune.	ETHLINE (Filiala vânzări)

Configurarea profil terminator L2TP pentru Sistem A

Dacă doriţi să configuraţi conexiunile la distanţă la staţii de lucru de la distanţă, trebuie să setaţi Sistem A să accepte conexiuni inbound de la aceşti clienţi.

Pentru a configura un profil terminator L2TP (Layer Two Tunneling Protocol) pentru Sistem A, finalizaţi următorii paşi:

1. Din System i Navigator, expandaţi ***Sistem A*** → **Reţea** → **Servicii de acces la distanţă**.
2. Faceţi clic dreapta pe **Profiluri conexiune receptor** pentru a seta Sistem A ca server care permite conexiuni inbound de la utilizatori la distanţă, şi selectaţi **Profil nou**.
3. Selectaţi următoarele opţiuni din pagina Setare:
   - **Tip protocol:** PPP
   - **Tio conexiune:** L2TP (linie virtuală)

     Notă: Câmpul **Mod de operare** ar trebui să afişeze automat **Terminator (server de reţea)**.
   - **Tip linie de serviciu:** Linie singulară
4. Faceţi clic pe **OK**. Astfel se va lansa pagina Proprietăţi profil nou punct-la-punct.
5. Pe fişa **General**, completaţi următoarele câmpuri:
   - **Nume**: MYCOL2TP
   - Selectaţi **Pornire profil cu TCP** dacă doriţi ca profilul să pornească automat cu TCP.
6. În fişa **Conexiune**, selectaţi **192.168.1.2** (**2001:DB8::2** în IPv6) pentru **Adresă IP punct final de tunel locală**.

   Important: Adresele IP folosite în acest scenariu sunt folosite doar ca exemplu. Ele nu reflectă o schemă de adrese IP şi nu ar trebui folosite în nici o configuraţie reală. Folosiţi propriile dumneavoastră adrese IP când completaţi aceste operaţii.
7. Selectaţi **MYCOL2TP** ca **Nume linie virtuală**. Astfel se va lansa pagina Proprietăţi nou L2TP.
8. În pagina Autentificare, introduceţi systema ca nume gazdă. Faceţi clic pe **OK**. Astfel veţi fi întors la pagina Conexiune.
9. În pagina Conexiune, selectaţi următoarele opţiuni şi introduceţi 25 ca **Număr maxim de conexiuni**.

a. Apăsaţi pe fişa **Autentificare** şi selectaţi **Cereţi acestui sistem să verifice identitatea sistemului la distanţă**.
b. Selectaţi **Autentificare locală cu lista de validare**.
c. Introduceţi QL2TP în câmpul **Nume listă de validare**, şi apăsaţi **Nou**.

10. În pagina Listă de validare, selectaţi **Adăugare**.
11. Adăugaţi nume de utilizatori şi parole pentru fiecare din angajaţii dumneavoastră la distanţă. Faceţi clic pe **OK**.
12. În pagina Confirmare parolă, re-introduceţi parola pentru fiecare angajat la distanţă. Apăsaţi **OK**.
13. În pagina Setare TCP/IP, selectaţi 10.1.1.1 (2001:DA8::1 în IPv6) pentru **Adresă IP locală**.
14. În câmpul **Metodă de asignare adresă IP**, selectaţi **Pool de adrese**.
15. În câmpul **Adresă IP de început**, introduceţi 10.1.1.100 şi 49 pentru **Număr de adrese**. Pentru adresă IPv6, în câmpul **Adresă IP de început**, introduceţi 2001:DA8::1:1 şi 65535 pentru **Număr de adrese**.
16. Selectaţi **Permitere sistemului de la distanţă să acceseze alte reţele (înaintare IP)**. Apăsaţi **OK**.

Pornire profil de conexiune receptor

După configurarea profilului de conexiune receptor L2TP (Layer Two Tunneling Protocol) pentru Sistem A, administratorul trebuie să pornească această conexiune astfel încât să asculte pentru cereri de intrare de la clienţi la distanţă.

Notă: S-ar putea să primiţi un mesaj de eroare pentru că subsistemul QUSRWRK nu este pornit. Acest mesaj apare la încercarea de pornire a profilului de conexiune receptor. Pentru a porni subsistemul QUSRWRK, urmaţi aceşti paşi:

1. Într-o interfaţă pe bază de caractere, introduceţi strsbs.
2. În ecranul Pornire subsistem, introduceţi QUSRWRK în câmpul **Descriere subsistem**.

Pentru a porni profilul de conexiune receptor pentru clienţi la distanţă, finalizaţi aceşti paşi:

1. În System i Navigator, selectaţi **Reîmprospătare** din meniul **Vizualizare**. Aceasta vă va reîmprospăta instanţa de System i Navigator.
2. În System i Navigator, expandaţi ***Sistem A*** → **Reţea** → **Servicii de acces la distanţă**.
3. Faceţi dublu clic pe **Profiluri de conexiune receptor** şi faceţi clic dreapta pe **MYCOL2TP** şi selectaţi **Pornire**.
4. Câmpul **Stare** va afişa, **Se aşteaptă cereri de conexiune**.

Configurare conexiune VPN pe Sistem A pentru clienţi la distanţă

După configurarea şi pornirea profilului de conexiune receptor L2TP (Layer Two Tunneling Protocol) pentru Sistem A, administratorul trebuie să configureze un VPN (virtual private network) pentru a proteja conexiunea dintre clienţi la distanţă şi reţeaua filialei de vânzări.

Pentru a configura un VPN pentru clienţi la distanţă, finalizaţi aceşti paşi:

Important: Adresele IP folosite în acest scenariu sunt folosite doar ca exemplu. Ele nu reflectă o schemă de adrese IP şi nu ar trebui folosite în nici o configuraţie reală. Folosiţi propriile dumneavoastră adrese IP când completaţi aceste operaţii.

1. Din System i Navigator, expandaţi ***Sistem A*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul VPN Conexiune nouă. Consultaţi pagina de Bun venit pentru informaţii despre ce obiecte creează vrăjitorul.
3. Apăsaţi **Următorul** pentru a vă duce la pagina Nume conexiune.
4. În câmpul **Nume**, introduceţi SalestoRemote.
5. Opţional: Specificaţi o descriere pentru acest grup conexiune. Apăsaţi **Următorul**.
6. În pagina Scenariu conexiune, selectaţi **Conectaţi gazda dvs. la altă gazdă**. Apăsaţi **Următorul**
7. În pagina Politica Internet Key Exchange, selectaţi **Creare politică nouă**, iar apoi selectaţi **Cea mai înaltă securitate, cea mai joasă performanţă**. Apăsaţi **Următorul**.
8. În pagina Certificat pentru Punct final de conexiune locală, selectaţi **Nu**. Apăsaţi **Următorul**.

9. În pagina Server de chei local, selectaţi **Adresă IP Versiunea 4** ca tip de identificator. Adresa IP asociată ar trebui să fie 192.168.1.2. Apăsaţi **Următorul**. Pentru adresa IPv6, în pagina Server de chei local, selectaţi **Adresă IP Versiunea 6** ca tip de identificator. Adresa IP asociată ar trebui să fie 2001:DB8::2. Apăsaţi **Următorul**.
10. În pagina Server de chei la distanţă, selectaţi **Orice adresă IP** din câmpul **Tip identificator**. În câmpul **Cheie pre-partajată**, introduceţi mycokey. Apăsaţi **Următorul**.
11. În pagina Servicii de date, introduceţi 1701 pentru portul local. Apoi selectaţi 1701 pentru portul la distanţă şi selectaţi **UDP** pentru protocol. Apăsaţi **Următorul**.
12. În pagina Politică de date, selectaţi **Creare politică nouă** şi apoi selectaţi **Cea mai înaltă securitate, cea mai joasă performanţă**. Apăsaţi **Următorul**.
13. În pagina Interfeţe aplicabile, selectaţi **ETHLINE**. Apăsaţi **Următorul**.
14. În pagina Rezumat, treceţi în revistă obiectele pe care vrăjitorul le va crea pentru a vă asigura că sunt corecte.
15. Apăsaţi pe **Sfârşit** pentru a termina configurarea. Când se deschide fereastra Activare filtre de politică, selectaţi **Nu, regulile de pachet vor fi activate mai târziu**. Apăsaţi **OK**.

Actualizare politici VPN pentru conexiuni la distanţă de la clienţi Windows XP şi Windows 2000

Deoarece vrăjitorul creează o conexiune standard care poate fi folosită pentru majoritatea configuraţiilor VPN (virtual private network), va trebui să actualizaţi politicile generate de către vrăjitor pentru a asigura interoperabilitatea cu clienţi Windows XP şi Windows 2000.

Pentru a actualiza aceste politici VPN, finalizaţi următoarele operaţii:

1. Din System i Navigator, expandaţi ***Sistem A*** **→ Reţea → Politici IP → Reţea privată virtuală → Politici de securitate IP**.
2. Faceţi dublu clic pe **Politici Internet Key Exchange** şi faceţi clic dreapta pe **Orice adresă IP** şi selectaţi **Proprietăţi**.
3. În pagina Transformare, apăsaţi **Adăugare**.
4. În pagina Adăugare transformare Internet Key Exchange, selectaţi următoarele opţiuni:
   - **Metodă de autentificare:** Cheie pre-partajată
   - **Algortim de dispersie:** MD5
   - **Algoritm de codare:** DES-CBC
   - **Grup Diffie-Hellman:** Grup 1
5. Faceţi clic pe **OK**.
6. Din System i Navigator, expandaţi ***Sistem A*** **→ Reţea → Politici IP → Reţea privată virtuală → Politici de securitate IP**.
7. Faceţi dublu clic pe **Politici de date** şi faceţi clic dreapta pe **SalestoRemote** şi selectaţi **Proprietăţi**.
8. În pagina General, curăţaţi **Folosire PFS (perfect forward secrecy) Diffie-Hellman**.
9. Selectaţi **Propunere ESP**, apăsaţi **Editare**.
10. În pagina Propunere politică de date, modificaţi opţiunile după cum urmează:
    - **Mod de încapsulare:** Transport
    - **Expirare cheie:** 15 minute
    - **Expirare la limita de dimensiune:** 100000
11. În pagina Transformare, apăsaţi **Adăugare**.
12. În pagina Adăugare transformare politică de date, selectaţi următoarele opţiuni:
    - **Protocol:** ESP (Encapsulating security payload)
    - **Algoritm de autentificare:** MD5
    - **Algoritm de codare:** DES-CBC
13. Apăsaţi **OK** de două ori.

Activare reguli de filtrare

Vrăjitorul creează automat regulile de pachete pe care această conexiune le cere pentru a funcţiona corespunzător. Totuşi, trebuie să le activaţi pentru ambele sisteme înainte de a porni conexiunea VPN (virtual private network).

Pentru a activa regulile de filtrare pentru Sistem A, urmaţi aceşti paşi:

Important: Adresele IP folosite în acest scenariu sunt folosite doar ca exemplu. Nu reflectă o schemă de adresare IP şi nu ar trebui folosite în nici o configuraţie reală. Trebuie să folosiţi propriile dumneavoastră adrese IP când completaţi aceste operaţii.

1. Din System i Navigator, expandaţi ***Sistem A*** → **Reţea** → **Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Activare reguli**.
3. Din pagina Activare reguli pachet, selectaţi **activare doar a regulilor generate VPN** şi selectaţi **ETHLINE** ca interfaţa pentru care doriţi să activaţi aceste reguli de filtre. Apăsaţi **OK**.

Înainte ca utilizatorii de la distanţă să îşi poată configura staţiile de lucru Windows XP, administratorul le furnizează următoarele informaţii astfel încât să îşi poată seta partea lor de conexiune. Pentru fiecare din utilizatorii dumneavoastră de la distanţă, daţi-le următoarele informaţii:

- Nume cheie pre-partajată: mycokey
- Adresa IP pentru Sistem A: 192.168.1.2 (2001:DB8::2 în IPv6)
- Nume de utilizator şi parolă pentru conexiune

Notă: Acestea au fost create când administratorul a adăugat numele de utilizator şi parolele într-o listă de validare în timpul configurării profilului terminator L2TP (Layer Two Tunneling Protocol).

Configurarea VPN pentru un client Windows XP

Folosiţi această procedură pentru a configura VPN pentru un clientWindows XP.

Utilizatorii de la distanţă de la MyCo, Inc trebuie să îşi seteze clientul la distanţăWindows XP prin completarea următorilor paşi:

1. În meniul Windows XP **Start**, expandaţi **All Programs** → **Accessories** → **Communications** → **New Connection Wizard**.
2. În pagina de Bun venit, citiţi informaţiile cu privire generală. Apăsaţi **Următorul**.
3. În pagina Tip de conexiune reţea, selectaţi **Conectare la reţeaua de la locul meu de muncă**. Apăsaţi **Următorul**.
4. În pagina Conexiune reţea, selectaţi **Conexiune Reţea privată virtuală (VPN)**. Apăsaţi **Următorul**.
5. În pagina Nume conexiune, introduceţi Conexiune la filială din câmpul **Nume companie**. Apăsaţi **Următorul**.
6. În pagina Reţea publică, selectaţi **Nu apelaţi conexiunea iniţială**. Apăsaţi **Următorul**.
7. În pagina Selectare server VPN, introduceţi 192.168.1.2 (2001:DB8::2 în IPv6) în câmpul **Nume gazdă sau adresă IP**. Apăsaţi **Următorul**.
8. În pagina Disponibilitate conexiune, selectaţi **Utilizat doar de mine**. Apăsaţi **Următorul**.
9. În pagina Rezumat, apăsaţi **Adăugaţi o scurtătură la această conexiune pe desktopul meu**. Faceţi clic pe **Sfârşit**.
10. Faceţi clic pe pictograma **Conectare Conexiune la MyCo** care a fost creată pe desktopul dumneavoastră.
11. În pagina Conectare Conexiune la MyCo, introduceţi numele de utilizator şi parola furnizate de administrator.
12. Selectaţi **Salvaţi acest nume de utilizator şi parolă pentru următorii utilizatori** şi **Doar eu**. Faceţi clic pe **Proprietăţi**.
13. În pagina **Securitate**, asiguraţi-vă că sunt selectate următoarele **Opţiuni de securitate**:
    - **Tipic**
    - **Necesită parolă securizată**
    - **Necesită criptare date**

    Faceţi clic pe **Setări IPSec**.

14. În pagina Setări IPSec, selectaţi **Folosire chei pre-partajate pentru autentificare** şi introduceţi mycokey în câmpul **Cheie pre-partajată**. Apăsaţi **OK**.
15. În pagina Lucru în reţea, selectaţi **VPN IPSec L2TP** ca **Tip de VPN**. Apăsaţi **OK**.
16. Semnaţi-vă cu nume de utilizator şi parolă şi faceţi clic pe **Conectare**.

Pentru a porni conexiunea VPN (virtual private network) din partea clientului, faceţi clic pe pictograma care apare pe desktopul dumneavoastră după finalizarea vrăjitorului de conexiune.

Testare conexiune VPN între puncte finale

După ce aţi terminat de configurat conexiunea între Sistem A şi utilizatori la distanţă şi aţi pornit cu succes conexiunea, ar trebui să testaţi conectivitatea pentru a vă asigura că gazdele la distanţă pot comunica între ele.

Pentru a testa conectivitatea, urmaţi aceşti paşi:

1. Din System i Navigator, expandaţi ***Sistem A*** → **Reţea**.
2. Faceţi clic dreapta pe **Configurarea TCP/IP** şi selectaţi **Utilitare** şi apoi selectaţi **Ping**.
3. Din dialogul **Ping de la**, introduceţi 10.1.1.101 (2001:DA8::1:101 în IPv6) în câmpul **Ping**.

   Notă: 10.1.1.101 reprezintă adresa IP asignată dinamic (pentru clientul de vânzări la distanţă) din pool-ul de adrese specificat în profilul terminator L2TP (Layer Two Tunneling Protocol) din System A.
4. Faceţi clic pe **Ping acum** pentru a verifica conectivitatea de la Sistem A la o staţie de lucru la distanţă. Faceţi clic pe **OK**.

Pentru a testa conexiunea de la clientul la distanţă, angajatul la distanţă urmează aceşti paşi de la o staţie de lucru pe care rulează Windows:

1. În promptul de comenzi, introduceţi ping 10.1.1.2 (ping 2001:DA8::2 în IPv6). Aceasta este adresa IP a unei staţii de lucru din reţeaua sediului central.
2. Repetaţi aceşti paşi pentru a testa conectivitatea de la sediul central la filială.

Scenariu: Folosire translatare adresă de reţea pentru VPN

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

Situaţie

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

Dată fiind natura confidenţială şi dependentă de timp a informaţiilor pe care le schimbaţi, vă decideţi să creaţi o reţea privată virtuală (VPN) între reţeaua furnizorului dumneavoastră şi reţeaua companiei dumneavoastră. Pentru a proteja şi mai mult confidenţialitatea structurii reţelei companiei dumneavoastră, decideţi că este nevoie să ascundeţi adresa IP privată a sistemului care găzduieşte aplicaţiile la care furnizorul are acces.

Puteţi folosi VPN nu numai pentru a crea definiţiile conexiunilor pe gateway-ul VPN din reţeaua companiei dumneavoastră, ci şi pentru a furniza translatarea de adrese de care aveţi nevoie pentru a ascunde adresele dumneavoastră locale private. Spre deosebire de translatarea adreselor de reţea (network address translation - NAT) convenţională, care modifică adresele IP din asocierile de securitate (security associations - SAs) de care are nevoie

VPN pentru a funcţiona, VPN NAT efectuează translatarea adreselor înainte de validarea SA, prin atribuirea unei adrese conexiunii în momentul în care aceasta este pornită.

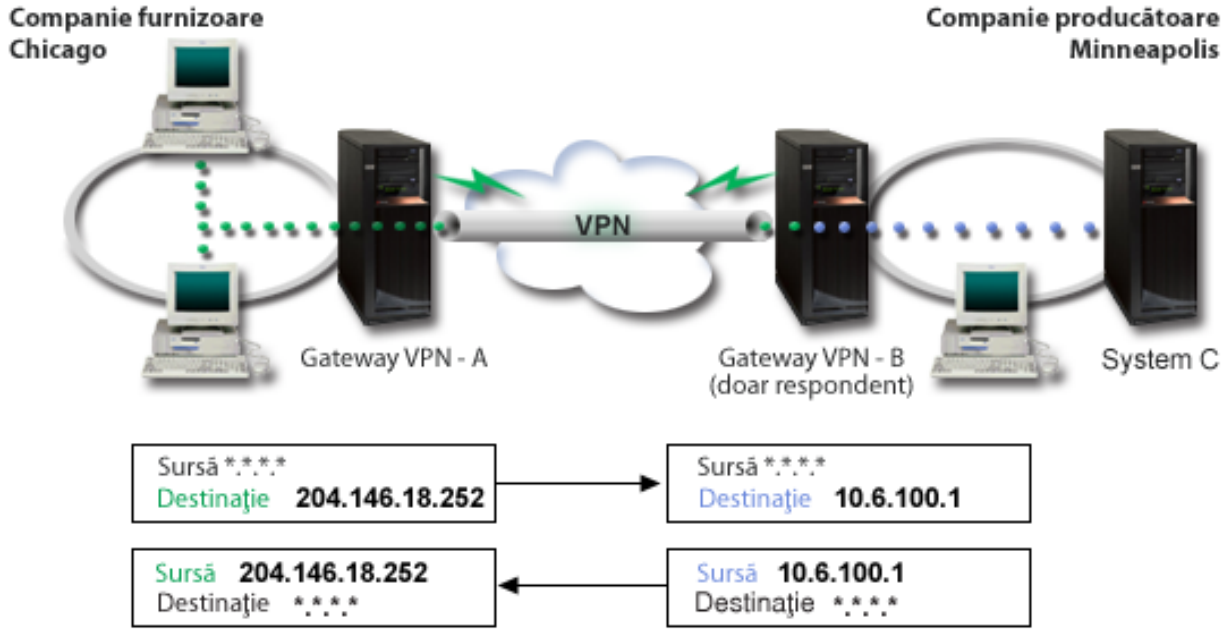
Obiective

Obiectivele acestui scenariu sunt:

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

Detalii

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



- VPN gateway-A este configurat pentru a iniţia întotdeauna conexiuni cu VPN gateway-B.
- VPN gateway-A defineşte punctul final de destinaţie al conexiunii ca 204.146.18.252 (adresa publică asignată pentru Sistem C).
- Sistem C are adresa IP privată în reţeaua producătorului 10.6.100.1.
- O adresă publică 204.146.18.252 a fost definită în pool-ul local de servicii din VPN gateway-B ca adresa privată pentru Sistem C, 10.6.100.1.
- VPN gateway-B translatează adresa publică pentru Sistem C la adresa sa privată, 10.6.100.1, pentru datagrame de intrare. VPN gateway-B translatează datagrame care se întorc, outbound, de la 10.6.100.1 înapoi la adresa publică a Sistem C, 204.146.18.252. În ceea ce îi priveşte pe clienţii din reţeaua furnizor, Sistem C are adresa IP 204.146.18.252. Ei nu îşi vor da seama că s-a produs o translatare a adresei.

Taskurile de configurare

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

1. Configuraţi un VPN gateway-la-gateway între **VPN gateway-A** şi **VPN gateway-B**.
2. Definiţi un pool de serviciu local în **VPN gateway-B** pentru a ascunde adresa privată a **System C** în spatele identificatorului public, 204.146.18.252.

3. Configuraţi **VPN gateway-B** pentru a translata adresele locale folosind adresele din pool-ul de serviciu local.

Concepte înrudite

"Translatarea adreselor de reţea pentru VPN" la pagina 8
VPN furnizează un mijloc pentru efectuarea de translatare a adreselor de reţea, denumit VPN NAT. VPN NAT diferă de NAT tradiţional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE şi IPSec. Studiaţi acest subiect pentru a afla mai multe.

Planificare pentru VPN

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

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

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

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

  Notă: Folosiţi consilierul de planificare VPN doar pentru conexiunile care suportă protocolul Internet Key Exchange (IKE). Pentru conexiunile dumneavoastră manuale, folosiţi foaia de lucru pentru planificarea conexiunilor manuale.
- Completarea foilor de lucru pentru planificarea VPN-ului

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

Operaţii înrudite

Folosirea consilierului de planificare VPN

"Configurarea VPN" la pagina 46
Interfaţa VPN vă furnizează câteva moduri diferite de configurare a conexiunilor dumneavoastră VPN. Puteţi configura o conexiune manuală sau dinamică.

Cerinţele pentru setarea VPN

Pentru ca o conexiune VPN să funcţioneze corect între sistemele dumneavoastră şi clienţi de reţea, trebuie să satisfaceţi cerinţele minime

Ce urmează este o listă a cerinţelor minime necesare pentru a seta o conexiune VPN:

Cerinţe sistem

- i5/OS Versiunea 5 Ediţia 3, sau mai nou
- Digital Certificate Manager
- System i Access pentru Windows
- System i Navigator
  - Componenta Reţea din System i Navigator
- Setaţi valoarea sistem reţinere date de securitate de pe server (QRETSVRSEC *SEC) la 1.
- TCP/IP trebuie să fie configurat, inclusiv interfeţe IP, rute, nume gazdă locală şi nume domeniu local.

Cerinţe client

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

Operaţii înrudite

“Iniţiere în depanarea VPN” la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Determinarea tipului de VPN care se va crea

Determinarea modului în care veţi folosi VPN este unul dintre primii paşi în planificarea cu succes. Pentru a face aceasta, trebuie să înţelegeţi rolul pe care îl joacă pentru conexiune atât serverul de chei local, cât şi serverul de chei la distanţă.

De exemplu, sunt punctele finale de *conexiune* diferite de punctele finale de *date*? Sunt aceleaşi sau vreo combinaţie a lor? Capetele conexiunii autentifică şi criptează (sau decriptează) traficul de date pentru conexiune şi furnizează (opţional) gestionarea cheilor cu protocolul Internet Key Exchange (IKE). Punctele finale de date, totuşi, definesc conexiunea dintre două sisteme pentru traficul IP care circulă prin VPN; de exemplu, tot traficul TCP/IP dintre 123.4.5.6 şi 123.7.8.9. În mod tipic, când capetele conexiunii şi capetele datelor sunt diferite, serverul VPN este un gateway. Când sunt aceleaşi, serverul VPN este un calculator gazdă.

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

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

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

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

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

Completarea fişei de lucru de planificare VPN

Folosiţi fişele de lucru de planificare VPN pentru a aduna informaţii detaliate despre planurile dumneavoastră de folosire VPN. Trebuie să completaţi aceste fişe de lucru pentru a vă planifica corespunzător strategia VPN. De asemenea, puteţi folosi aceste informaţii pentru a vă configura VPN-ul.

Dacă preferaţi, puteţi tipări şi completa fişele de lucru de planificare pentru a aduna informaţii detaliate despre planurile dumneavoastră de folosire VPN.

Alegeţi fişa de lucru pentru tipul de conexiune pe care doriţi să o creaţi.

- Fişă de lucru de planificare pentru conexiuni dinamice
- Fişă de lucru pentru planificare pentru conexiuni manuale
- Consilier planificare VPN

  Sau, dacă preferaţi, folosiţi consilierul pentru planificare interactivă şi pentru îndrumare la configurare. Consilierul de planificare vă pune întrebări despre reţeaua dumneavoastră şi, pe baza răspunsurilor dumneavoastră, vă furnizează sugestii pentru crearea VPN-ului dumneavoastră.

  Notă: Folosiţi consilierul de planificare VPN doar pentru conexiunile dumneavoastră dinamice. Folosiţi fişa de lucru de planificare pentru conexiuni manuale pentru tipurile dumneavoastră de conexiuni manuale.

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

Informaţii înrudite

Consilier planificare VPN

Fişă de lucru pentru planificare pentru conexiuni dinamice

Completaţi această fişă de lucru înainte de a configura o conexiune dinamică.

Înainte de a vă crea conexiunile dinamice VPN, completaţi această fişă de lucru. Fişa de lucru presupune că veţi folosi vrăjitorul Conexiune nouă. Vrăjitorul vă permite să setaţi un VPN pe baza cerinţelor dumneavoastră primare de securitate. În unele cazuri, s-ar putea să fie nevoie să rafinaţi proprietăţile pe care vrăjitorul le configurează pentru o conexiune. De exemplu, s-ar putea să consideraţi ca aveţi nevoie de jurnalizare sau că doriţi ca serverul VPN să pornească de fiecare dată când porneşte TCP/IP. În acest caz, faceţi clic dreapta pe grupul sau conexiunea de grup dinamic creată de vrăjitor şi selectaţi **Proprietăţi**.

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

Tabela 9. Cerinţele sistemului

Listă de verificare pentru cerinţele preliminare	**Răspunsuri**
Sistemul dumneavoastră de operare este i5/OS V5R3, sau mai nou?	Da
Este instalată opţiunea Digital Certificate Manager?	Da
Este instalat System i Access pentru Windows?	Da
Este instalat System i Navigator?	Da
Este instalată subcomponenta Reţea din System i Navigator?	Da
Este instalat IBM TCP/IP Connectivity Utilities for i5/OS?	Da
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	Da
Este configurat TCP/IP pe sistem (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	Da
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	Da
Aţi aplicat cele mai recente corecţii temporare de program (PTF-uri)?	Da
Dacă tunelul VPN traversează firewall-uri sau rutere care utilizează filtrarea pachet IP, regulile de filtru ale firewall-ului sau ale ruterului suportă protocoalele AH şi ESP?	Da
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele IKE (UDP port 500), AH şi ESP?	Da

Tabela 9. Cerinţele sistemului (continuare)

Listă de verificare pentru cerinţele preliminare	Răspunsuri
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	Da

Tabela 10. Configuraţia VPN

Aveţi nevoie de aceste informaţii pentru a configura o conexiune dinamică VPN	Răspunsuri
Ce tip de conexiune creaţi? • Gateway-la-gateway • Gazdă-la-gateway • Gateway-la-gazdă • Gazdă-la-gazdă	
Cum veţi denumi grupul de chei dinamice?	
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile? • Cea mai bună securitate, cele mai mici performanţe • Echilibrare securitate şi performanţă • Cea mai joasă securitate şi cea mai bună performanţă	
Folosiţi 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 distanţă ?	
Care este identificatorul punctului final de date la distanţă ?	
De ce tip de securitate şi performanţe ale sistemului aveţi nevoie pentru a vă proteja cheile? • Cea mai bună securitate, cele mai mici performanţe • Echilibrare securitate şi performanţă • Cea mai joasă securitate şi cea mai bună performanţă	

Fişă de lucru pentru planificare pentru conexiuni manuale

Completaţi această fişă de lucru înainte de a configura o conexiune manuală.

Completaţi această fişă de lucru pentru a vă ajuta la crearea conexiunilor dumneavoastră VPN (virtual private network) care nu folosesc IKE pentru gestionarea cheilor. Răspundeţi la fiecare din aceste întrebări înainte de a continua cu setarea VPN:

Tabela 11. Cerinţe sistem

Listă de verificare cerinţe preliminare	Răspunsuri
Sistemul rulează i5/OS V5R3, sau mai nou?	
Este instalat Digital Certificate Manager?	
Este instalat System i Access pentru Windows?	
Este instalat System i Navigator?	
Este instalată subcomponenta Reţea din System i Navigator?	
Este instalat IBM TCP/IP Connectivity Utilities for i5/OS?	
Aţi setat la 1 valoarea de sistem pentru reţinerea datelor de securitate ale serverului (QRETSVRSEC *SEC)?	
Este configurat TCP/IP pe sistem (inclusiv interfeţele IP, rutele, numele de gazdă locală şi numele de domeniu local)?	
Este stabilită comunicaţia TCP/IP normală între punctele finale cerute?	

Tabela 11. Cerinţe sistem (continuare)

Aţi aplicat cele mai recente corecţii 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 şi ESP?	
Sunt configurate firewall-urile sau ruterele pentru a permite protocoalele AH şi ESP?	
Sunt configurate firewall-urile pentru a permite înaintarea (forwarding) IP?	

Tabela 12. Configuraţia VPN

Aveţi nevoie de aceste informaţii pentru a configura manual un VPN	**Răspunsuri**
Ce tip de conexiune creaţi? • Gazdă-la-gazdă • Gazdă-la-gateway • Gateway-la-gazdă • Gateway-la-gateway	
Cum veţi denumi conexiunea?	
Care este identificatorul capătului local al conexiunii?	
Care este identificatorul capătului la distanţă al conexiunii?	
Care este identificatorul punctului final de date local ?	
Care este identificatorul punctului final de date la distanţă ?	
Ce tip de trafic veţi permite pentru această conexiune (port local, port la distanţă şi protocol)?	
Aveţi nevoie de translatare de adrese pentru această conexiune? Consultaţi Translatarea adreselor de reţea pentru VPN pentru informaţii suplimentare.	
Veţi folosi modul tunel sau modul transport?	
Ce protocol IPSec va folosi conexiunea (AH, ESP sau AH cu ESP)? Consultaţi Securitate IP (IPSec) pentru informaţii suplimentare.	
Ce algoritm de autentificare va folosi conexiune (HMAC-MD5 sau HMAC-SHA)?	
Ce algoritm de criptare va folosi conexiunea (DES-CBC sau 3DES-CBC)? **Notă:** Specificaţi un algoritm de criptare numai dacă aţi selectat ESP ca protocol IPSec.	
Care este cheia inbound AH? Dacă folosiţi MD5, cheia este un şir hexazecimal de 16 octeţi. Dacă folosiţi SHA, cheia este un şir hexazecimal de 20 de octeţi. Cheia dumneavoastră inbound trebuie să corespundă exact cheii outbound a serverului de la distanţă.	
Care este cheia outbound AH? Dacă folosiţi MD5, cheia este un şir hexazecimal de 16 octeţi. Dacă folosiţi SHA, cheia este un şir hexazecimal de 20 de octeţi. Cheia dumneavoastră outbound trebuie să corespundă exact cheii inbound a serverului de la distanţă.	
Care este cheia inbound ESP? Dacă folosiţi DES, cheia este un şir hexazecimal de 8 octeţi. Dacă folosiţi 3DES, cheia este un şir hexazecimal de 24 de octeţi. Cheia dumneavoastră inbound trebuie să corespundă exact cheii outbound a serverului de la distanţă.	
Care este cheia outbound ESP? Dacă folosiţi DES, cheia este un şir hexazecimal de 8 octeţi. Dacă folosiţi 3DES, cheia este un şir hexazecimal de 24 de octeţi. Cheia dumneavoastră outbound trebuie să corespundă exact cheii inbound a serverului de la distanţă.	
Care este Indexul politicii de securitate inbound (SPI)? SPI inbound este un şir hexazecimal de 4 octeţi, unde primul octet este setat la 00. SPI-ul dumneavoastră inbound trebuie să corespundă exact cu SPI-ul outbound al serverului de la distanţă.	

Tabela 12. Configuraţia VPN (continuare)

Care este SPI-ul outbound? SPI outbound este un şir hexazecimal de 4 octeţi. SPI-ul dumneavoastră outbound trebuie să corespundă exact cu SPI-ul inbound al serverului de la distanţă.	

Concepte înrudite

“Translatarea adreselor de reţea pentru VPN” la pagina 8
VPN furnizează un mijloc pentru efectuarea de translatare a adreselor de reţea, denumit VPN NAT. VPN NAT diferă de NAT tradiţional prin aceea că translatează adresele înainte de aplicarea protocoalelor IKE şi IPSec. Studiaţi acest subiect pentru a afla mai multe.

Configurarea VPN

Interfaţa VPN vă furnizează câteva moduri diferite de configurare a conexiunilor dumneavoastră VPN. Puteţi configura o conexiune manuală sau dinamică.

O conexiune dinamică este una care generează şi negociază dinamic cheile care vă securizează conexiunea, în timp ce este activă, prin utilizarea protocolului IKE (Internet Key Exchange). Conexiunile dinamice furnizează un nivel în plus de securitate pentru datele care o traversează din cauza schimbării cheilor, automat, la intervale regulate. În consecinţă, este puţin probabil că un atacator poate să captureze o cheie, să aibă timp să o spargă, şi să o folosească la dirijarea sau capturarea traficului pe care cheia îl protejează.

O conexiune manuală, totuşi, nu oferă suport pentru negocieri IKE şi în consecinţă, gestionare automată de chei. Mai departe, amândouă terminările de conexiune necesită să le configuraţi diferite atribute care trebuie să se potrivească exact. Conexiunile manuale folosesc chei statice care nu se reîmprospătează sau schimbă atâta timp cât conexiunea este activă. Trebuie să opriţi o conexiune manuală pentru a schimba cheile sale asociate. Dacă consideraţi acest lucru un risc de securitate, aţi putea crea o conexiune dinamică în schimb.

Concepte înrudite

“Planificare pentru VPN” la pagina 41
Primul pas în utilizarea cu succes a VPN-ului este planificarea. Acest subiect furnizează informaţii despre migrarea de la ediţiile anterioare, cerinţele de setare şi legături către un consilier de planificare care va genera o foaie de lucru personalizată pentru specificaţiile dumneavoastră.

Configurare conexiuni VPN cu vrăjitorul Conexiune nouă

Vrăjitorul de conexiune nouă vă permite să creaţi o reţea privată virtuală (VPN) între orice combinaţie de gazdă şi gateway.

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

Vrăjitorul creează automat fiecare obiect de configuraţie de care VPN are nevoie pentru a funcţiona corespunzător, inclusiv regulile de pachete. Totuşi, dacă trebuie să adăugaţi funcţii la VPN-ul dumneavoastră; de exemplu, jurnalizare sau VPN NAT (network address translation for VPN - translatare adresă de reţea pentru VPN), s-ar putea să doriţi să vă îmbunătăţiţi mai departe VPN-ul prin fişele de proprietăţi ale conexiunii sau grupului dinamic de chei corespunzător. Pentru aceasta, trebuie să opriţi întâi conexiunea dacă este activă. Apoi faceţi clic dreapta pe grupul de chei dinamice sau conexiune şi selectaţi **Proprietăţi**.

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Conexiune nouă** pentru a porni vrăjitorul.

3. Finalizaţi vrăjitorul pentru a crea o conexiune VPN de bază. Faceţi clic pe **Ajutor**, dacă aveţi nevoie de ajutor.

Operaţii înrudite

Consilier planificare VPN

Configurare politici de securitate VPN

După ce determinaţi cum veţi folosi VPN-ul, trebuie să vă definiţi politicile de securitate pentru VPN.

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

Operaţii înrudite

"Configurarea unei conexiuni VPN securizată" la pagina 48
După ce aţi configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configuraţi conexiunea sigură.

Configurarea unei politici Schimbare de chei Internet (IKE)

Politica IKE (Internet Key Exchange) defineşte ce nivel de protecţie de autentificare şi criptare foloseşte IKE în faza 1 a negocierilor.

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

VPN foloseşte fie modul semnătură RSA, fie chei prepartajate pentru a autentifica negocierile de fază 1. Dacă doriţi să folosiţi certificate digitale pentru autentificarea serverelor de chei, trebuie mai întâi să le configuraţi prin utilizarea Digital Certificate Manager. Politica IKE de asemenea identifică ce server de chei la distanţă va folosi această politică.

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

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

Se recomandă să utilizaţi negocierea în modul principal de fiecare dată când este utilizată o cheie prepartajată pentru autentificare. În acest fel, schimbul este mai sigur. Dacă trebuie să utilizaţi chei prepartajate şi negocierea mod agresiv, selectaţi parole pentru care este puţin probabil să fie sparte în atacurile care scanează dicţionarul. Se recomandă de asemenea să vă modificaţi periodic parolele. Pentru a forţa un schimb de chei să utilizeze negocierea în mod principal, executaţi următoarele operaţii:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Selectaţi **VPN → Politici de securitate IP → Politici Internet Key Exchange** pentru a vedea politicile de schimb chei definite curent în panoul din dreapta.
3. Faceţi clic dreapta pe o anumită politică de schimb de chei şi selectaţi **Proprietăţi**.
4. În pagina Transformare, faceţi clic pe **Politică răspuns**. Apare dialogul Politică Internet Key Exchange respondent.
5. În câmpul Protecţie identitate, deselectaţi **Negociere în mod agresiv IKE (fără protecţie identitate)**.
6. Faceţi clic pe **OK** pentru a vă întoarce în dialogul Proprietăţi.
7. Apăsaţi **OK** din nou pentru a salva modificările.

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

Concepte înrudite

"Gestionarea cheilor" la pagina 6
Un VPN dinamic furnizează securitate suplimentară pentru comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.

Operaţii înrudite

Digital Certificate Manager

Configurarea unei politici de date

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

Sistemele care comunică cad de acord asupra acestor atribute în timpul negocierilor din faza 2 a protocolului Internet Key Exchange (IKE). Nu este nevoie să definiţi o politică de date când creaţi o conexiune manuală. În plus, dacă vă creaţi VPN-ul cu vrăjitorul Conexiune nouă, acesta poate crea politica de date în locul dumneavoastră.

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

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

Concepte înrudite

"Gestionarea cheilor" la pagina 6
Un VPN dinamic furnizează securitate suplimentară pentru comunicaţiile dumneavoastră prin folosirea protocolului Internet Key Exchange (IKE) pentru gestionarea cheilor. IKE permite serverelor VPN de la fiecare capăt al conexiunii să negocieze chei noi la intervale specificate.

Configurarea unei conexiuni VPN securizată

După ce aţi configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configuraţi conexiunea sigură.

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

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

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

Pentru a configura obiectul conexiune securizată, executaţi atât taskurile din Partea întâi, cât şi cele din Partea a doua.

Concepte înrudite

"Configurare politici de securitate VPN" la pagina 47
După ce determinaţi cum veţi folosi VPN-ul, trebuie să vă definiţi politicile de securitate pentru VPN.

"Configurare reguli pachet VPN" la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Operaţii înrudite

"Activare reguli pachet VPN" la pagina 54
Trebuie să activaţi regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Partea întâi: Configurarea unui grup de chei dinamice

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**.
2. Faceţi clic dreapta pe **După grup** şi selectaţi **Grup nou de chei dinamice**.
3. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Partea a doua: Configurarea unei conexiuni chei dinamice

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

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

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

Configurarea unei conexiuni manuale

O conexiune manuală este una pentru care trebuie să configuraţi toate proprietăţile VPN fără să folosiţi vrăjitori.

Mai mult, ambele capete ale conexiunii vă cer să configuraţi câteva elemente care trebui să se potrivească *exact*. De exemplu, cheile dumneavoastră inbound trebuie să se potrivească cu cheile outbound ale sistemului de la distanţă, altfel conexiunea va eşua.

Conexiunile manuale folosesc chei statice care nu sunt reîmprospătate sau schimbate cât timp conexiunea este activă. Trebuie să opriţi o conexiune manuală pentru ai schimba cheie asociată. Dacă consideraţi acest lucru un risc de securitate şi ambele capete ale conexiunii suportă protocolul IKE (Internet Key Exchange), s-ar putea să doriţi să luaţi în calcul setarea unei conexiuni dinamice.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → → Conexiuni securizate**.
2. Faceţi clic dreapta pe **Toate conexiunile** şi selectaţi **Conexiune manuală nouă**.

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

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

Operaţii înrudite

"Configurarea unei reguli de filtrare politici" la pagina 52
Efectuaţi acest task doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile de filtrare politici automat.

Configurarea unei conexiuni dinamice

O conexiune dinamică generează şi negociază dinamic cheile care vă securizează conexiunea, în timp ce este activă, prin utilizarea protocolului IKE (Internet Key Exchange).

Finalizaţi vrăjitorul Conexiune nouă cu chei dinamică pentru a configura o conexiune dinamică prin urmarea acestor paşi:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate → După grup**.
2. Faceţi clic dreapta pe grupul specific de chei dinamic şi selectaţi **Conexiune nouă cu chei dinamică**.
3. Completaţi fiecare tabel de proprietăţi. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** pentru a salva modificările.

Configurare reguli pachet VPN

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

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

În general, VPN cere două tipuri de reguli de filtrare: reguli de filtrare Pre-IPSec şi reguli de filtrare de politici. Revedeţi subiectele de mai jos pentru a afla cum se configurează aceste reguli folosind editorul de reguli de pachete din System i Navigator. Dacă vreţi să citiţi despre alte opţiuni VPN şi de filtrare, vedeţi secţiunea Filtrare VPN şi 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 acţiune IPSEC. Acest subiect discută doar despre regulile pre-IPSec cerute de VPN pentru a funcţiona corespunzător. În acest caz, regulile pre-IPSec sunt o pereche de reguli care permit procesarea IKE peste conexiune. IKE permite ca generarea şi negocierea dinamică de chei să aibă loc pe conexiunea dumneavoastră. S-ar putea să fie nevoie adăugaţi alte reguli pre-IPSec în funcţie de mediul dumneavoastră de reţea şi politica de securitate.

  Notă: Trebuie să configuraţi acest tip de regulă pre-IPSec doar dacă aveţi deja alte reguli care permit IKE pentru sisteme specifice. Dacă nu există reguli de filtrare special pentru permiterea traficului IKE, atunci acesta este implicit permis.
- Configurarea unei reguli filtrare politici

  Regula de filtrare politică defineşte traficul care poate folosi VPN şi ce politică de protecţie a datelor să se aplice acestui trafic.

Lucruri de luat în seamă înainte de a începe

Când adăugaţi reguli de filtrare pentru a interfaţă, sistemul adaugă automat o regulă implicită de negare pentru acea interfaţă. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteţi şi nu puteţi schimba această regulă. Ca rezultat, s-ar putea să observaţi că traficul care funcţiona în mod misterios va eşua după ce vă activaţi regulile de filtrare VPN. Dacă doriţi să permiteţi alt trafic decât VPN prin interfaţă, trebuie să adăugaţi reguli explicite de permitere.

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

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

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

Concepte înrudite

“VPN şi filtrarea IP” la pagina 11
Filtrarea IP şi VPN sunt foarte înrudite. De fapt, majoritatea conexiunilor VPN necesită reguli de filtrare pentru a funcţiona corect. Acest subiect vă oferă informaţii despre ce filtre necesită VPN, împreună cu alte concepte de filtrare înrudite cu VPN.

Operaţii înrudite

“Configurarea unei conexiuni VPN securizată” la pagina 48
După ce aţi configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configuraţi conexiunea sigură.

“Configurarea regulii de filtrare pre-IPSec”
Efectuaţi această operaţie doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile filtrare politică automat.

“Configurarea unei reguli de filtrare politici” la pagina 52
Efectuaţi acest task doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile de filtrare politici automat.

“Definirea unei interfeţe pentru regulile de filtrare VPN” la pagina 53
După ce v-aţi configurat regulile pachet VPN şi orice alte reguli de care aveţi nevoie, pentru a vă activa conexiunea VPN trebuie să definiţi interfaţa la care se aplică.

“Activare reguli pachet VPN” la pagina 54
Trebuie să activaţi regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Configurarea regulii de filtrare pre-IPSec

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru sistemul dumneavoastră.
3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare → Filtru**.

5. În pagina **General**, specificaţi un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puţin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică şi unul pentru regulile de filtru PERMIT şi DENY. Numiţi setul care conţine regulile dumneavoastră de filtru pre-IPSec cu prefixul *preipsec*. De exemplu, preipsecfilters.
6. În câmpul **Acţiune**, selectaţi **PERMIT** din lista derulantă.
7. În câmpul **Direcţie**, selectaţi **OUTBOUND** din lista derulantă.
8. În câmpul **Nume adresă sursă**, selectaţi **=** din prima listă derulantă şi apoi introduceţi adresa IP a serverului local de chei în al doilea câmp. Aţi specificat adresa IP a serverului local de chei în politica IKE.
9. În câmpul **Nume adresă destinaţie**, selectaţi **=** din prima listă derulantă şi apoi introduceţi adresa IP a serverului la distanţă de chei în al doilea câmp. Aţi specificat de asemenea adresa IP a serverului la distanţă de chei în politica IKE.
10. În pagina **Servicii**, selectaţi **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**.
11. În câmpul **Protocol**, selectaţi **UDP** din lista derulantă.
12. Pentru **Portul sursă**, selectaţi **=** în primul câmp, apoi introduceţi 500 în al doilea câmp.
13. Repetaţi pasul anterior pentru **Portul destinaţie**.
14. Faceţi clic pe **OK**.
15. Repetaţi aceşti paşi pentru a configura filtrul INBOUND. Folosiţi acelaşi nume de set şi inversaţi adresele dacă e nevoie.

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

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

Concepte înrudite

“Configurare reguli pachet VPN” la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Operaţii înrudite

“Configurarea unei reguli de filtrare politici”
Efectuaţi acest task doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile de filtrare politici automat.

Configurarea unei reguli de filtrare politici

Efectuaţi acest task doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile de filtrare politici automat.

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru sistemul dumneavoastră.
3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare → Filtru**.
5. În pagina **General**, specificaţi un nume de set pentru regulile dumneavoastră de filtrare VPN. Se recomandă crearea a cel puţin trei seturi diferite: unul pentru regulile de filtru pre-IPSec, unul pentru regulile dumneavoastră de filtru politică şi unul pentru regulile de filtru PERMIT şi DENY. De exemplu, policyfilters

6. În câmpul **Acţiune**, selectaţi **IPSEC** din lista derulantă. Câmpul **Direcţie** este implicit pe OUTBOUND şi nu puteţi să-l schimbaţi. Deşi acest câmp este implicit pe OUTBOUND, este de fapt bi-direcţional. Apare OUTBOUND pentru a clarifica semantica valorilor inbound. De exemplu, valorile sursă sunt valori locale şi valorile destinaţie sunt valori la distanţă.
7. Pentru **Nume adresă sursă**, selectaţi **=** în primul câmp şi apoi introduceţi adresa IP a punctului final local de date în al doilea câmp. Puteţi de asemenea să specificaţi un interval de adrese IP sau o adresă IP plus o mască de subreţea după ce le definiţi folosind funcţia **Definire Adrese**.
8. Pentru **Nume adresă destinaţie**, selectaţi **=** în primul câmp şi apoi introduceţi adresa IP a punctului final la distanţă de date în al doilea câmp. Puteţi de asemenea să specificaţi un interval de adrese IP sau o adresă IP plus o mască de subreţea după ce le definiţi folosind funcţia **Definire Adrese**.
9. În câmpul **Jurnalizare**, specificaţi ce nivel de jurnalizare aveţi nevoie.
10. În câmpul **Nume conexiune**, selectaţi definiţia conexiunii la care se aplică aceste reguli de filtrare.
11. (opţional) Introduceţi o descriere.
12. În pagina **Servicii**, selectaţi **Service**. Aceasta activează câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**.
13. În câmpurile **Protocol**, **Port sursă** şi **Port destinaţie**, selectaţi valoarea corespunzătoare pentru trafic. Sau, puteţi selecta asteriscul (*) din lista derulantă. Aceasta permite oricărui protocol care foloseşte orice port să folosească VPN.
14. Faceţi clic pe **OK**.

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

Notă: Când adăugaţi reguli de filtrare pentru o interfaţă, sistemul adaugă automat o regulă implicită de negare pentru acea interfaţă. Această înseamnă că orice trafic care nu este în mod explicit permis este negat. Nu puteţi şi nu puteţi schimba această regulă. Ca rezultat, s-ar putea să observaţi că acele conexiuni care funcţionau în mod misterios vor ceda după ce activaţi regulile de filtrare VPN. Dacă doriţi să permiteţi alt trafic decât VPN prin interfaţă, trebuie să adăugaţi reguli explicite de permitere.

Concepte înrudite

“Configurare reguli pachet VPN” la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Operaţii înrudite

“Configurarea unei conexiuni manuale” la pagina 49
O conexiune manuală este una pentru care trebuie să configuraţi toate proprietăţile VPN fără să folosiţi vrăjitori.

“Configurarea regulii de filtrare pre-IPSec” la pagina 51
Efectuaţi această operaţie doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile filtrare politică automat.

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

Definirea unei interfeţe pentru regulile de filtrare VPN

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

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Editor reguli**. Aceasta deschide editorul Reguli pachet, care vă permite să creaţi sau să editaţi filtre şi reguli NAT pentru sistemul dumneavoastră.

3. În fereastra Bine aţi venit, selectaţi **Creare fişier regulă pachet nou** şi faceţi clic pe **OK**.
4. Din editorul Reguli pachet selectaţi **Inserare → Interfaţă filtru**.
5. În pagina **General**, selectaţi **Nume linie** şi apoi selectaţi din lista derulantă descrierea liniei la care se aplică regulile pachet VPN.
6. (opţional) Introduceţi o descriere.
7. În pagina **Seturi filtre**, apăsaţi **Adăugare** pentru a adăuga fiecare nume de set pentru filtrele pe care tocmai le-aţi configurat.
8. Faceţi clic pe **OK**.
9. Salvaţi fişierul cu regulile dumneavoastră. Fişierul este salvat în sistemul de fişiere integrat de pe sistemul dumneavoastră cu extensia .i3p.

   Notă: Nu vă salvaţi fişierul în următorul director:

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

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

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

Concepte înrudite

"Configurare reguli pachet VPN" la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Operaţii înrudite

"Configurarea unei reguli de filtrare politici" la pagina 52
Efectuaţi acest task doar dacă aţi specificat că nu vreţi ca VPN să vă genereze regulile de filtrare politici automat.

"Activare reguli pachet VPN"
Trebuie să activaţi regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

Activare reguli pachet VPN

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

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

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

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

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

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

Concepte înrudite

"Configurare reguli pachet VPN" la pagina 50
Dacă creaţi o conexiune pentru prima dată, permiteţi-i VPN-ului să genereze automat regulile pachet VPN pentru dumneavoastră. Puteţi face asta fie folosind vrăjitorul de Conexiune nouă, fie folosind pagina de proprietăţi pentru a vă configura conexiunea.

Operaţii înrudite

"Configurarea unei conexiuni VPN securizată" la pagina 48
După ce aţi configurat politicile de securitate pentru conexiunea dumneavoastră, trebuie apoi să configuraţi conexiunea sigură.

"Definirea unei interfeţe pentru regulile de filtrare VPN" la pagina 53
După ce v-aţi configurat regulile pachet VPN şi orice alte reguli de care aveţi nevoie, pentru a vă activa conexiunea VPN trebuie să definiţi interfaţa la care se aplică.

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

Configurare confidenţialitate flux de trafic (TFC)

Dacă politica dumneavoastră de date este configurată pentru modul de tunel puteţi folosi TFC (traffic flow confidentiality) pentru a ascunde lungimea reală a pachetelor de date transferate printr-o conexiune VPN.

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

Pentru a activa TFC pe o conexiune VPN, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi serverul dumneavoastră **> Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate → Toate conexiunile**.
2. Faceţi clic dreapta pe conexiunea pe care vreţi să activaţi TFC şi selectaţi **Proprietăţi**.
3. În fişa **General** selectaţi **Folosire TFC (Traffic Flow Confidentiality) în modul Tunel**.

Configurare număr de ordine extins

Puteţi folosi ESN (extended sequence number) pentru a mări rata de transfer a datelor unei conexiuni VPN.

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

Pentru a activa ESN pe o conexiune VPN, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală**
2. Faceţi clic dreapta pe **Reţea privată virtuală** şi selectaţi **Proprietăţi**.
3. În fişa **General** selectaţi **Folosire ESN (Extended Sequence Number)**.

Pornirea unei conexiuni VPN

Finalizaţi această operaţie pentru a porni conexiuni pe care le iniţiaţi local.

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

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

Operaţii înrudite

"Activare reguli pachet VPN" la pagina 54
Trebuie să activaţi regulile pachet VPN înainte de a vă putea porni conexiunile VPN.

"Iniţiere în depanarea VPN" la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Gestionare VPN

Puteţi folosi interfaţa în System i Navigator pentru a vă manipula toate operaţiile de gestionare VPN cum sunt, oprirea unei conexiuni şi vizualizarea atributelor de conexiune.

Utilizaţi interfaţa VPN din System i Navigator pentru a manipula toate taskurile de gestiune, inclusiv:

Setare atribute implicite pentru conexiunile dumneavoastră

Valorile implicite apar în panourile pe care le folosiţi să creaţi noi politici şi conexiuni. Puteţi seta valori implicite pentru nivelurile de securitate, pentru administrarea sesiunilor de chei, pentru duratele de viaţă ale cheilor şi pentru duratele de viaţă ale conexiunilor.

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic pe **Reţea privată virtuală** şi selectaţi **Valori implicite**.
3. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.
4. Apăsaţi **OK** după ce aţi completat fiecare fişă de proprietăţi.

Resetarea conexiunilor în stare de eroare

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o resetaţi şi selectaţi **Resetare**. Aceasta resetează conexiunea la starea inactiv. Pentru a reseta mai multe conexiuni care sunt în stare de eroare, selectaţi fiecare conexiune pe care doriţi să o resetaţi, faceţi clic dreapta şi selectaţi **Resetare**.

Vizualizare informaţii de eroare

Finalizaţi această operaţie pentru a vă ajuta în a determina de ce conexiunea dumneavoastră provoacă o eroare.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea eronată pe care vreţi să o vedeţi şi selectaţi **Informaţii despre eroare**.

Operaţii înrudite

"Iniţiere în depanarea VPN" la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Vizualizare atribute de la conexiuni active

Finalizaţi această operaţie pentru a verifica starea şi alte atribute ale conexiunilor dumneavoastră active.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea activă sau la cerere pe care doriţi să o vizualizaţi şi selectaţi **Proprietăţi**.
4. Mergeţi la pagina **Atribute curente** pentru a vedea atributele conexiunii.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Din meniul **Obiecte**, selectaţi **Coloane**. Aceasta deschide o casetă de dialog care vă permite să selectaţi care atribute vreţi să le afişaţi în fereastra System i Navigator.

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

Concepte înrudite

"Mesaje de eroare comune ale managerului de conexiune VPN" la pagina 71
Managerul de conexiune VPN înregistrează în istoric două mesaje în istoricul de job QTOVMAN când apare o eroare la o conexiune VPN.

Vizualizare urmărire server VPN

Vă permite să configuraţi, să porniţi, să opriţi şi să vizualizaţi urmăririle server VPN Connection Manager şi VPN Key Manager. Acesta este similar cu folosirea comenzii TRCTCPAPP *VPN din interfaţa bazată pe caractere cu excepţia că puteţi vedea urmărirea cât timp o conexiune este activă.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **VPN**, selectaţi **Unelte de diagnosticare** şi **Urmărire server**.

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

1. Din fereastra **Urmă de legare la reţea privată virtuală**, apăsaţi pe  (Opţiuni).
2. În pagina **Manager conexiuni**, specificaţi ce tip de urmărire doriţi să ruleze serverul Connection Manager.
3. În pagina **Manager chei**, specificaţi ce tip de urmărire doriţi să ruleze serverul Key Manager.
4. Apăsaţi **Ajutor** dacă aveţi întrebări despre cum să completaţi o pagină sau oricare din câmpurile ei.

5. Apăsaţi **OK** pentru a salva modificările.
6. Apăsaţi  (Pornire) pentru a porni urmărirea. Apăsaţi pe  (Reîmprospătare) în mod periodic pentru a vedea cele mai recente informaţii de urmărire.

Vizualizare istorice de job server VPN

Urmaţi aceste instrucţiuni pentru a vedea fişierele jurnal de joburi din VPN Key Manager şi VPN Connection Manager.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reţea privată virtuală**, selectaţi **Unelte de diagnoză** şi apoi selectaţi istoricul jobului de server pe care doriţi să-l vizualizaţi.

Vizualizare atribute pentru Asocieri de securitate

Finalizaţi această operaţie pentru a afişa 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, urmaţi paşii de mai jos:

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea activă corespunzătoare şi selectaţi **Asocieri de securitate**. Fereastra rezultată vă permite să vizualizaţi proprietăţile fiecărei dintre SA-urile asociate cu o conexiune specifică.

Oprirea unei conexiuni VPN

Finalizaţi această operaţie pentru a opri conexiuni active.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o opriţi şi selectaţi **Oprire**. Pentru a opri mai multe conexiuni, selectaţi fiecare conexiune pe care doriţi să o opriţi, faceţi clic dreapta şi selectaţi **Oprire**.

Ştergere obiecte de configurare VPN

Înainte să ştergeţi un obiect de configurare VPN din baza de date de politici VPN, asiguraţi-vă că înţelegeţi cum afectează alte conexiuni şi grupuri de conexiuni VPN.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**
2. Apăsaţi **Toate conexiunile** pentru a afişa o listă a conexiunilor în panoul din dreapta.
3. Faceţi clic dreapta pe conexiunea pe care vreţi să o ştergeţi şi selectaţi **Ştergere**.

Depanarea VPN

Folosiţi următoarele metode de depanare pentru a rezolva unele probleme de bază pe care le-aţi putea întâlni în timpul configurării unei conexiuni VPN.

VPN este o tehnologie complexă care se schimbă rapid şi care necesită cel puţin cunoştinţe de bază privind tehnologiile IPSec obişnuite. Trebuie de asemenea să fiţi familiarizat cu regulile pachet IP deoarece VPN necesită câteva reguli filtru pentru a funcţiona corect. Din cauza acestei complexităţi, s-ar putea, din când în când, să întâmpinaţi probleme cu conexiunile dumneavoastră VPN. Depanarea VPN nu este întotdeauna o sarcină uşoară. Trebuie să vă înţelegeţi mediile de reţea şi de sistem, cât şi componentele pe care le folosiţi când obişnuiţi să le gestionaţi. Următoarele subiecte vă furnizează indicaţii pentru depanarea diverselor probleme pe care le-aţi putea întâlni în timpul folosirii VPN:

Iniţiere în depanarea VPN

Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Există câteva moduri de a începe analizarea problemelor VPN:

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

Concepte înrudite

"Cerinţele pentru setarea VPN" la pagina 41
Pentru ca o conexiune VPN să funcţioneze corect între sistemele dumneavoastră şi clienţi de reţea, trebuie să satisfaceţi cerinţele minime

"Depanarea VPN cu istoricele de job VPN" la pagina 70
Când aveţi probleme la conexiunile dumneavoastră VPN, este întotdeauna recomandabil să istoricele de job. De fapt există câteva istorice de job care conţin mesaje de eroare şi alte informaţii legate de un mediu VPN.

"Depanarea VPN cu urmele de comunicaţii" la pagina 75
IBM i5/OS furnizează capabilitatea de urmărire a datelor pe o linie de comunicaţie, cum ar fi o interfaţă reţea locală (LAN) sau reţea pe zonă extinsă (WAN). Utilizatorul obişnuit s-ar putea să nu înţeleagă tot conţinutul datelor de urmărire. Oricum, puteţi folosi intrările de urmărire pentru a determina dacă un schimb de date între sistemele la distanţă şi local a avut loc.

Operaţii înrudite

"Vizualizare informaţii de eroare" la pagina 56
Finalizaţi această operaţie pentru a vă ajuta în a determina de ce conexiunea dumneavoastră provoacă o eroare.

"Depanarea VPN cu jurnalul QIPFILTER" la pagina 65
Vedeţi aceste informaţii pentru a afla despre regulile de filtrare VPN.

"Pornirea unei conexiuni VPN" la pagina 55
Finalizaţi această operaţie pentru a porni conexiuni pe care le iniţiaţi local.

Alte lucruri de verificat

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

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

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

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

Notă: Ar putea fi rutere sau firewall-uri intermediare care realizează filtrare de pachet IP care ar putea filtra pachetele PING. PING este bazat de obicei pe protocolul ICMP. Dacă PING reuşeşte, ştiţi că există legătura. Dacă PING nu reuşeşte, ştiţi doar că a eşuat PING. Aţi putea încerca alte protocoale IP între cele două sisteme, cum ar fi Telnet sau FTP pentru a verifica conectivitatea.

2. Verificaţi regulile de filtrare pentru VPN şi asiguraţi-vă că sunt activate. Porneşte filtrarea cu bine? Dacă răspundeţi **da**, treceţi la pasul 3. Dacă răspundeţi **nu**, verificaţi mesajele de eroare din fereastra Reguli pachet din System i Navigator. Asiguraţi-vă că regulile de filtrare nu specifică Translatarea Adreselor de Reţea (NAT) pentru traficul VPN.
3. Porniţi conexiunea dumneavoastră VPN. Porneşte conexiunea cu bine? Dacă răspundeţi **da**, mergeţi la pasul 4. Dacă răspundeţi **nu**, verificaţi istoricele de job QTOVMAN şi QTOKVPNIKE pentru erori. Când folosiţi VPN-ul, furnizorul dumneavoastră de servicii Internet (ISP) şi fiecare gateway de securitate din reţeaua dumneavoastră trebuie să suporte protocoalele Authentication Header (AH) şi Encapsulated Security Payload (ESP). Dacă alegeţi să folosiţi AH sau ESP depinde de propunerile pe care le definiţi pentru conexiunile dumneavoastră VPN.
4. Puteţi activa o sesiune utilizator peste conexiunea VPN? Dacă răspundeţi **da**, atunci conexiunea VPN funcţionează aşa cum aţi cerut. Dacă răspundeţi **nu**, atunci verificaţi regulile pachet şi grupurile cheie dinamică VPN şi conexiunile pentru definiţiile filtru care nu permit traficul utilizator pe care îl vreţi.

Erorile obişnuite de configurare VPN şi cum se pot repara

Folosiţi aceste informaţii pentru a examina mesaje de eroare VPN obişnuite şi pentru a le învăţa posibilele rezolvări.

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

Mesaj de eroare VPN: TCP5B28

Când încercaţi să activaţi reguli de filtrare pe o interfaţă, ajungeţi la acest mesaj: TCP5B28 CONNECTION_DEFINITION order violation

Simptom:

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

```
TCP5B28: Violare ordine CONNECTION_DEFINITION
```

Soluţia posibilă:

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

Mesaj de eroare VPN : Articolul nu a fost găsit

Când faceţi clic dreapta pe un obiect VPN şi selectaţi fie **Proprietăţi** sau **Ştergere**, ajungeţi la mesajul care spune **Articol negăsit**.

Simptom:

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

Soluţia posibilă:

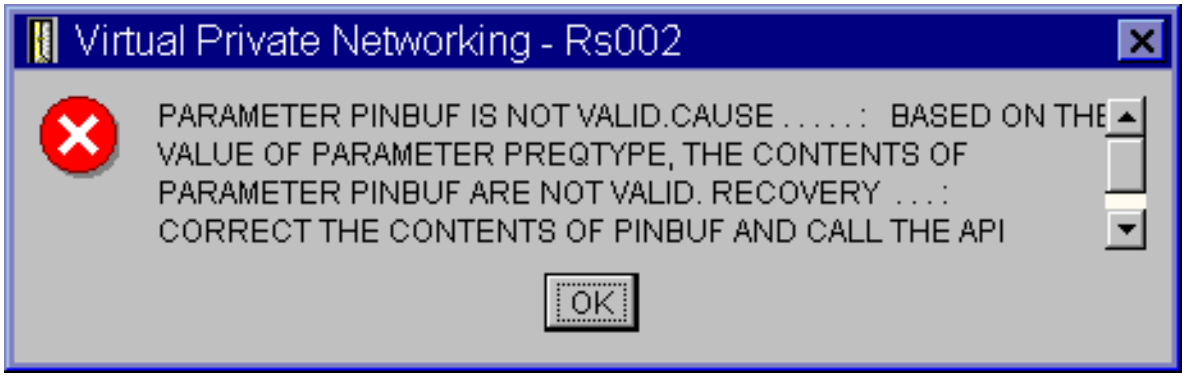
- S-ar putea să fi şters sau redenumit obiectul, şi nu aţi reîmprospătat încă fereastra. Ca urmare, obiectul apare încă în fereastra Reţea privată virtuală. Pentru a verifica dacă este aşa, din meniul **Vizualizare**, selectaţi **Reîmprospătare**. Dacă obiectul apare tot în fereastra Reţea privată virtuală,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

Mesaj de eroare VPN: Parametrul PINBUF nu este valid

Când încercaţi să realizaţi o conexiune, ajungeţi la mesajul care spune: **PARAMETER PINBUF IS NOT VALID...**

Simptom:

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



Soluţia posibilă:

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

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

Când selectaţi **Proprietăţi** pentru o conexiune de chei dinamice, ajungeţi la o eroare care spune că serverul nu poate găsi serverul de chei la distanţă specificat de dumneavoastră.

Simptom:

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

Soluţia posibilă:

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

Mesaj de eroare VPN: Nu se poate actualiza obiectul

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

Simptom:

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

Soluţia posibilă:

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

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

Ajungeţi 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:

Soluţia posibilă:

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

Concepte înrudite

"Eroare VPN: Toate cheile sunt goale"
Când vizualizaţi proprietăţile unei conexiuni manuale, toate cheile prepartajate şi cheile algoritmului pentru conexiune sunt goale.

Mesaj de eroare VPN: CPF9821

Când încercaţi să expandaţi sau să deschideţi containerul Politici IP din System i Navigator, apare mesajul CPF9821- Fără autorizaţie la programul QTFRPRS din bilioteca QSYS.

Simptom:

Când încercaţi să expandaţi sau să deschideţi containerul Politici IP dinSystem i Navigator, apare mesajul CPF9821- Fără autorizaţie la programul QTFRPRS din bilioteca QSYS.

Soluţia posibilă:

S-ar putea să nu aveţi autorizarea necesară pentru a extrage starea curentă de la Reguli pachet sau de la manager conexiune VPN. Asiguraţi-vă că aveţi autorizare *IOSYSCFG pentru a avea acces la funcţiile Reguli pachet din System i Navigator.

Eroare VPN: Toate cheile sunt goale

Când vizualizaţi proprietăţile unei conexiuni manuale, toate cheile prepartajate şi cheile algoritmului pentru conexiune sunt goale.

Simptom:

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

Soluţia posibilă:

Aceasta se întâmplă când valoarea de sistem QRETSVRSEC este setată înapoi la 0. Setarea acestei valori de sistem la 0 şterge toate cheile din baza de date a politicii VPN. Pentru a rezolva această problemă trebuie să setaţi valoarea de sistem la 1 şi apoi să reintroduceţi toate cheile. Consultaţi Mesaj de eroare: Nu se pot cripta cheile pentru informaţii suplimentare despre cum se realizează aceasta.

Concepte înrudite

"Mesaj de eroare VPN: Nu se poate cripta cheia..." la pagina 62
Ajungeţi 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 folosiţi Reguli pachet

Prima dată când folosiţi interfaţa de reguli pachete în System i Navigator, un ecran de deschidere de sesiune apare pentru un sistem diferit de cel curent.

Simptom:

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

Soluţia posibilă:

Reguli pachet foloseşte unicode pentru a memora regulile de securitate pachet în sistemul de fişiere integrat. Înregistrarea suplimentară permite System i Access pentru Windows să obţină tabela de conversie corespunzătoare pentru unicode. Aceasta se va întâmpla doar o dată.

Eroare VPN: Valoare goală de stare conexiune în fereastra System i Navigator

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

Simptom:

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

Soluţia 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 reîmprospătaţi fereastra, conexiunea va afişa o stare de Eroare, Activă, La-cerere sau Inactivă.

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

După ce opriţi o conexiune, fereastra System i Navigator arată conexiunea încă activă.

Simptom:

După ce opriţi o conexiune, fereastra System i Navigator arată conexiunea încă activă.

Soluţia posibilă:

Aceasta se întâmplă de obicei pentru că nu aţi reîmprospătat fereastra System i Navigator. Astfel, fereastra conţine informaţii vechi. Pentru a repara aceasta, de la meniul **Vizualizare**, selectaţi **Reîmprospătare**.

Eroare VPN : 3DES nu este o soluţie pentru criptare

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

Simptom:

Când lucraţi 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.

Soluţia posibilă:

Cel mai probabil, aveţi instalat doar produsul Cryptographic Access Provider (5722-AC2) pe sistemul dumneavoastră, şi nu Cryptographic Access Provider (5722-AC3). Cryptographic Access Provider (5722-AC2) permite doar algoritmul de criptare DES (Data Encryption Standard) datorită restricţiilor la lungimea cheilor. Cryptographic Access Provider (5722-AC2) şi (5722-AC3) nu mai sunt necesare pentru activarea criptării datelor pe sisteme pe care rulează i5/OS V5R4, sau mai nou.

Eroare VPN: Afişare neaşteptată de coloane în fereastra System i Navigator

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

Simptom:

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

Soluţia posibilă:

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

Eroare VPN: Regulile de filtrare active nu pot fi dezactivate

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

Simptom:

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

Soluţia posibilă:

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

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

Când creaţi o conexiune cu cheie dinamică, specificaţi un grup de chei dinamice şi un identificator pentru serverul de chei la distanţă. Mai târziu, când vedeţi proprietăţile obiectului conexiunii înrudite, pagina General a foii de proprietăţi afişează acelaşi identificator de server de chei la distanţă, dar un grup de chei dinamice diferit.

Simptom:

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

Soluţia posibilă:

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

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

Depanarea VPN cu jurnalul QIPFILTER

Vedeţi aceste informaţii pentru a afla despre regulile de filtrare VPN.

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

Operaţii înrudite

“Iniţiere în depanarea VPN” la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Activarea jurnalului QIPFILTER

Utilizaţi editorul Reguli pachet din System i Navigator pentru a activa jurnalul QIPFILTER.

Trebuie să activaţi funcţia de înregistrare în istoric pentru fiecare regulă filtru în parte. Nu există nici o funcţie care permite înregistrarea în istoric pentru toate datagramele IP care intră sau ies din sistem.

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

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP**.
2. Faceţi clic dreapta pe **Reguli pachet** şi selectaţi **Configurare**. Aceasta afişează interfaţa Reguli pachet.
3. Deschideţi un fişier cu reguli de filtrare existent.

4. Faceţi dublu clic pe regula de filtrare pe care doriţi s-o jurnalizaţi.
5. Pe pagina **General**, selectaţi **FULL** în câmpul **Jurnalizare** ca în caseta de dialog de mai sus. Aceasta activează înregistrarea în istoric pentru această regulă de filtrare.
6. Faceţi clic pe **OK**.
7. Salvaţi şi activaţi fişierul modificat cu regula de filtrare.

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

Folosirea jurnalului QIPFILTER

i5/OS creează automat jurnalul prima oară când activaţi filtrarea pachet IP.

Pentru a vedea detaliile specifice-intrării din jurnal, puteţi afişa intrările din jurnal pe ecran sau puteţi folosi un fişier de ieşire. Copiind intrările din jurnal în fişierul de ieşire, puteţi vedea cu uşurinţă intrările folosind utilitare de interogare aşa cum este Query/400 sau SQL. Puteţi de asemenea să vă scrieţi propriile programe HLL pentru a procesa intrările din fişierele de ieşire.

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

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

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

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

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

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

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

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

Concepte înrudite

“Câmpurile din jurnalul QIPFILTER”
Examinaţi următoarea tabelă care descrie câmpurile din fişierul de ieşire QIPFILTER

Câmpurile din jurnalul QIPFILTER

Examinaţi următoarea tabelă care descrie câmpurile din fişierul de ieşire QIPFILTER

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TFENTL	5	Y	Lungimea intrării	
TFSEQN	10	Y	Număr de ordine	
TFCODE	1	N	Cod jurnal	Întotdeauna M
TFENTT	2	N	Tip intrare	Întotdeauna TF
TFTIME	26	N	Amprentă de timp SAA	
TFJOB	10	N	Nume job	

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TFUSER	10	N	Profil utilizator	
TFNBR	6	Y	Număr job	
TFPGM	10	N	Nume program	
TFRES1	51	N	Rezervat	
TFUSPF	10	N	Utilizator	
TFSYMN	8	N	Nume sistem	
TFRES2	20	N	Rezervat	
TFRESA	50	N	Rezervat	
TFLINE	10	N	Descriere linie	*ALL dacă TFREVT este U*, spaţiu dacă TFREVT este L*, Nume linie dacă TFREVT este L
TFREVT	2	N	Eveniment regulă	L* sau L când regulile sunt încărcate. U* când regulile sunt descărcate, A la acţiune filtru
TFPDIR	1	N	Direcţie pachet IP	O este ieşire, I este intrare
TFRNUM	5	N	Număr regulă	Se aplică la numărul regulii din fişierul activ de reguli
TFACT	6	N	Acţiunea filtru efectuată	PERMIT, DENY sau IPSEC
TFPROT	4	N	Protocol transport	1 este ICMP 6 este TCP 17 este UDP 50 este ESP 51 este AH
TFSRCA	15	N	Adresa IP sursă	
TFSRCP	5	N	Port sursă	Gunoi dacă TFPROT= 1 (ICMP)
TFDSTA	15	N	Adresa IP destinaţie	
TFDSTP	5	N	Port destinaţie	Gunoi dacă TFPROT= 1 (ICMP)
TFTEXT	76	N	Text suplimentar	Conţine descriere dacă TFREVT= L* sau U*

Operaţii înrudite

“Folosirea jurnalului QIPFILTER” la pagina 66
i5/OS creează automat jurnalul prima oară când activaţi filtrarea pachet IP.

Depanarea VPN cu jurnalul QVPN

Furnizează informaţii despre traficul IP şi despre conexiuni.

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

Activarea jurnalului QVPN

Utilizaţi interfaţa reţea privată virtuală din System i Navigator pentru a activa jurnalul VPN.

Nu există nici o funcţie care permite înregistrarea în jurnal pentru toate conexiunile VPN. De aceea, trebuie să activaţi funcţia de înregistrare în istoric pentru fiecare grup cheie dinamic sau conexiune manuală.

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

1. În System i Navigator, expandaţi **sistemul dumneavoastră → Reţea → Politici IP → Reţea privată virtuală → Conexiuni securizate**.
2. Pentru grupuri de chei dinamice, expandaţi **După grup** şi apoi faceţi clic dreapta pe grupul de chei dinamice pentru care doriţi să activaţi jurnalizarea şi selectaţi **Proprietăţi.**
3. Pentru conexiuni manuale, expandaţi **Toate conexiunile** şi apoi faceţi clic dreapta pe conexiunea manuală pentru care doriţi să activaţi jurnalizarea.
4. În pagina **General**, selectaţi nivelul de jurnalizare pe care îl cereţi. Aveţi de ales dintre patru opţiuni. Acestea sunt:

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

   Toate Jurnalizarea se realizează pentru toate activităţile conexiunii, cum ar fi pornirea sau oprirea unei conexiuni sau reîmprospătarea unei chei, cât şi pentru informaţiile despre traficul IP.

   Activitate conexiune
   Jurnalizarea se realizează pentru o activitate a conexiunii, cum ar fi pornirea sau oprirea unei conexiuni.

   Trafic IP
   Jurnalizarea se realizează pentru tot traficul VPN care este asociat cu această conexiune. Este făcută o intrare în jurnal de fiecare dată când o regulă filtru este invocată. Sistemul înregistrează informaţii despre traficul IP în jurnalul QIPFILTER, care se află în biblioteca QUSRSYS.
5. Faceţi clic pe **OK**.
6. Porniţi conexiunea pentru a activa jurnalizarea.

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

Folosirea jurnalului QVPN

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

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

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

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

.

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

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

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

Concepte înrudite

"Câmpurile din jurnalul QVPN"
Examinaţi următoarea tabelă care descrie câmpurile din fişierul de ieşire QVPN

Câmpurile din jurnalul QVPN

Examinaţi următoarea tabelă care descrie câmpurile din fişierul de ieşire QVPN

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TSENTL	5	Y	Lungimea intrării	
TSSEQN	10	Y	Număr de ordine	
TSCODE	1	N	Cod jurnal	Întotdeauna M
TSENTT	2	N	Tip intrare	Întotdeauna TS
TSTIME	26	N	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	
TSCMPN	10	N	Componenta VPN	
TSCONM	40	N	Nume conexiune	
TSCOTY	10	N	Tip conexiune	
TSCOS	10	N	Stare conexiune	
TSCOSD	8	N	Data de pornite	
TSCOST	6	N	Timpul pornirii	
TSCOED	8	N	Data de sfârşit	
TSCOET	6	N	Timpul de sfârşit	
TSTRPR	10	N	Protocol transport	
TSLCAD	43	N	Adresa locală a clientului	
TSLCPR	11	N	Porturi locale	
TSRCAD	43	N	Adresa de la distanţă a clientului	
TSCPR	11	N	Porturi de la distanţă	
TSLEP	43	N	Punct final local	

Nume câmp	Lungime câmp	Numeric	Descriere	Comentarii
TSREP	43	N	Punct final la distanţă	
TSCORF	6	N	Număr de reîmprospătări	
TSRFDA	8	N	Data următoarei reîmprospătări	
TSRFTI	6	N	Timpul următoarei reîmprospătări	
TSRFLS	8	N	Durata de viaţă a reîmprospătării	
TSSAPH	1	N	Faza SA	
TSAUTH	10	N	Tip autentificare	
TSENCR	10	N	Tip criptare	
TSDHGR	2	N	Grup Diffie-Hellman	
TSERRC	8	N	Cod eroare	

Operaţii înrudite

“Folosirea jurnalului QVPN” la pagina 68
Pentru a vedea detaliile specifice-intrării din jurnalul VPN, puteţi afişa intrările din jurnal pe ecran sau puteţi folosi un fişier de ieşire.

Depanarea VPN cu istoricele de job VPN

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

Este important să analizaţi istoricele de job de la ambele părţi ale conexiunii dacă ambele părţi sunt modele System i. Când o conexiune dinamică nu poate porni, este folositor să înţelegeţi ce se întâmplă pe serverul de la distanţă.

Joburile VPN, QTOVMAN şi QTOKVPNIKE, rulează în subsistemul QSYSWRK. Puteţi să vizualizaţi istoricele de job corespunzătoare din System i Navigator.

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

QTCPIP
Acest job este jobul de bază care porneşte toate interfeţele TCP/IP. Dacă aveţi probleme fundamentale cu TCP/IP în general, analizaţi 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 conţine mesaje pentru fiecare încercare de conectare care eşuează.

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

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

QTPPPL2TP

Acesta este jobul manager pentru L2TP (Layer Two Tunneling Protocol). Dacă aveţi probleme la configurarea unui tunel L2TP, vedeţi mesajele din acest istoric de job.

Operaţii înrudite

"Iniţiere în depanarea VPN" la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Mesaje de eroare comune ale managerului de conexiune VPN

Managerul de conexiune VPN înregistrează în istoric două mesaje în istoricul de job QTOVMAN când apare o eroare la o conexiune VPN.

Primul mesaj furnizează detalii cu privire la eroare. Puteţi vedea informaţii despre aceste erori în System i Navigator făcând clic dreapta pe conexiunea cu eroare şi selectând **Informaţii eroare**.

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

Mesajele de eroare ale managerului de conexiune VPN

Mesaj	Cauză	Recuperare
TCP8601 Nu s-a putut porni conexiunea VPN [*nume conexiune*]	Nu s-a putut porni această conexiune VPN datorită unui sau mai multe coduri motiv: *0* - Un mesaj anterior din istoricul de joburi cu acelaşi nume de conexiune VPN are mai multe informaţii detaliate. *1* - Configurarea politicii VPN. *2* - Eşuarea reţelei de comunicaţii. *3* - Managerul de chei VPN a eşuat în a negocia o nouă asociere de securitate. *4* - Punctul final la distanţă pentru această conexiune nu este configurat corespunzător. *5* - Managerul de chei VPN a eşuat să răspundă managerului de conexiune VPN. *6* - Eşuare de încărcare a conexiunii VPN a componentei de securitate IP. *7* - Eşuare componentă PPP.	1. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi System i Navigator pentru a vizualiza starea conexiunii. Conexiunile care nu au putut fi pornite for fi în stare de eroare.
TCP8602 Eroarea a apărut la oprirea conexiunii VPN [*nume conexiune*]	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 acelaşi nume de conexiune VPN are mai multe informaţii detaliate. *1* - Conexiunea VPN nu există. *2* - Eşuare de comunicaţii internă cu managerul de chei VPN. *3* - Eşuare de comunicaţii internă cu componenta IPSec. *4* - Eşuare de comunicaţii cu punctul final la distanţă de conexiune VPN.	1. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi System i Navigator 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	Cauză	Recuperare
TCP8604 Pornirea conexiunii VPN [*nume conexiune*] a eşuat	O pornire a acestei conexiuni VPN a eşuat datorită unuia din următoarele coduri eroare: *1* - Nu s-a putut translata numele de gazdă la distanţă 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 iniţială pentru conexiunea VPN nu permite specificarea acţiunii. *6* - Un rol sistem pentru conexiunea VPN este inconsistent în informaţii de la grupul de conexiune. *7* - Rezervat. *8* - Punctele finale de date (servicii şi adrese la distanţă şi locale) a acestei conexiuni VPN sunt inconsistente în informaţii de la grupul de conexiune. *9* - Tipul identificator nu este valid.	1. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi System i Navigator pentru a verifica sau corecta configuraţia de politică VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.
TCP8605 Managerul de conexiune VPN nu a putut 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. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Verificaţi dacă interfaţa *LOOPBACK este activă folosind comanda NETSTAT OPTION(*IFC). 3. Terminaţi serverul VPN folosind comanda ENDTCPSVR SERVER(*VPN). Apoi reporniţi serverul VPN folosind comanda STRTCPSRV SERVER(*VPN). **Notă:** Aceasta provoacă toate conexiunile VPN să se termine.
TCP8606 Managerul de chei VPN nu a putut stabili asocierea de securitate cerută pentru conexiunea [*nume conexiune*]	Managerul de chei VPN nu a putut stabili asocierea de securitate cerută datorită unuia din următoarele coduri eroare: *24* - A eşuat autentificarea de către managerul de chei VPN a cheii conexiunii. *8300* - Eşuarea a apărut în timpul negocierilor de chei ale conexiunii managerului de chei VPN. *8306* - Nu s-a găsit nici o cheie prepartajată. *8307* - Nu s-a găsit nici o politică de fază 1 IKE la distanţă. *8308* - Nu s-a găsit nici o cheie prepartajată la distanţă. *8327* - E expirat timpul negocierilor de chei de conexiune a managerului de chei VPN. *8400* - Eşuare apărută în timpul negocierilor de conexiune VPN ale managerului de chei Key VPN. *8407* - Nu s-a găsit nici o politică de fază 2 IKE la distanţă. *8408* - E expirat timpul de negocieri de conexiune VPN ale managerului de chei VPN. *8500 sau 8509* - A apărut o eroare de reţea la managerul de chei VPN.	1. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi System i Navigator pentru a verifica sau corecta configuraţia de politică VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile.

Mesajele de eroare ale managerului de conexiune VPN

Mesaj	Cauză	Recuperare
TCP8608 Conexiunea VPN, [*nume conexiune*], nu a putut obţine o adresă NAT	Acest grup de chei dinamice sau conexiune de date au specificat că translatarea de adresă reţea (NAT) e făcută pe una sau mai multe adrese şi că a eşuat datorită unuia dintre posibilele coduri motiv: *1* - Adresa căruia trebuie să i se aplice NAT nu este o adresă IP singulară. *2* - Toate adresele disponibile au fost folosite.	1. Verificaţi istoricul de joburi pentru mesaje adiţionale. 2. Corectaţi erorile şi încercaţi cererea din nou. 3. Folosiţi System i Navigator pentru a verifica sau corecta politica VPN. Asiguraţi-vă că grupul de chei dinamice asociat cu această conexiune are configurate valori acceptabile pentru adrese.
TCP8620 Nu este disponibil punctul final de conexiune local.	Nu s-au putut activa aceste conexiuni VPN pentru că punctul final de conexiune locală nu a fost disponibil.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Asiguraţi-vă că punctul final de conexiune local este definit şi pornit folosind comanda NETSTAT OPTION(*IFC). 3. Corectaţi orice erori şi încercaţi 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. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Asiguraţi-vă că punctul final de conexiune local este definit şi pornit folosind comanda NETSTAT OPTION(*IFC). 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8622 Încapsularea de transport nu este permisă cu un gateway	Nu s-a putut activa această conexiune VPN pentru că politica negociată a specificat modul de încapsulare de transport şi această conexiune este definită ca un gateway de securitate.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a schimba politica VPN asociată cu această conexiune VPN. 3. Corectaţi orice erori şi încercaţi 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 [*valoarea punctului final de date local*] şi un punct final de date la distanţă de [*valoarea punctului final de date la distanţă*].	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a vizualiza toate conexiunile activate care au puncte finale de date locale şi puncte finale de date la distanţă care se suprapun peste conexiune. Schimbaţi politica unei conexiuni existente dacă amândouă conexiunile sunt necesare. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Mesajele de eroare ale managerului de conexiune VPN

Mesaj	Cauză	Recuperare
TCP8624 Conexiunea VPN nu este în domeniul regulii de filtrare a politii asociate	Nu s-a putut activa această conexiune VPN pentru că punctele finale de date nu sunt în regula de filtrare a politicii definite.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a afişa restricţiile 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 verificaţi punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acţiune IPSEC şi un nume de conexiune VPN asociat cu această conexiune. Schimbaţi politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8625 Conexiunea VPN e eşuat la o verificare de algoritm ESP	Nu s-a putut activa această conexiune VPN din cauza insuficienţei cheii secrete asociată cu conexiunea.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a afişa politica asociată cu această conexiune şi introduceţi o cheie secretă diferită. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8626 Punctul final al conexiunii VPN nu este acelaşi cu punctul final de date.	Nu s-a putut activa această conexiune VPN pentru că politica specifică o gazdă existentă şi punctul final de conexiune VPN nu este acelaşi lucru cu punctul final de date.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a afişa restricţiile 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 verificaţi punctele finale de date ale conexiunii. Acestea trebuie să se încadreze în regula de filtre activă care are o acţiune IPSEC şi un nume de conexiune VPN asociat cu această conexiune. Schimbaţi politica de conexiune existentă sau regula de filtrare pentru a activa această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Mesajele de eroare ale managerului de conexiune VPN

Mesaj	Cauză	Recuperare
TCP8628 Regula de filtrare politici nu este încărcată	Regula de filtrare politici pentru această conexiune nu este activă.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a afişa filtrele de politici active. Verificaţi regula de filtrare politici pentru această conexiune. 3. Corectaţi orice erori şi încercaţi cererea din nou.
TCP8629 Pachet IP abandonat pentru conexiunea VPN	Această conexiune VPN are VPN NAT configurat şi setul cerut de adrese NAT a depăşit adresele disponibile NAT.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Folosiţi System i Navigator pentru a creşte numărul de adrese NAT atribuite pentru această conexiune VPN. 3. Corectaţi orice erori şi încercaţi 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 eşuare a apărut.	1. Verificaţi istoricele de joburi pentru mesaje adiţionale de aplicat acestei conexiuni. 2. Verificaţi istoricul de joburi asociat cu conexiunea PPP. 3. Corectaţi orice erori şi încercaţi cererea din nou.

Operaţii înrudite

“Vizualizare atribute de la conexiuni active” la pagina 57
Finalizaţi această operaţie pentru a verifica starea şi alte atribute ale conexiunilor dumneavoastră active.

Depanarea VPN cu urmele de comunicaţii

IBM i5/OS furnizează capabilitatea de urmărire a datelor pe o linie de comunicaţie, cum ar fi o interfaţă reţea locală (LAN) sau reţea pe zonă extinsă (WAN). Utilizatorul obişnuit s-ar putea să nu înţeleagă tot conţinutul datelor de urmărire. Oricum, puteţi folosi intrările de urmărire pentru a determina dacă un schimb de date între sistemele la distanţă şi local a avut loc.

Pornirea urmăririi de comunicaţii

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

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

Parametrii de comandă sunt explicaţi în lista următoare:

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

CFGTYPE (Tip de configurare)
E urmărită o linie (*LIN), o interfaţă reţea (*NWI) sau un server de reţea (*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). Prin urmare, aţi putea primi un mesaj de eroare la folosirea unei dimensiuni de buffer mai mare pentru comanda STRCMNTRC decât cea definită în SST. Ţineţi minte că suma dimensiunilor de buffer specificate pe toate urmăririle de comunicaţii pornite nu trebuie să depăşească dimensiunea maximă de buffer definită în SST.

DTADIR (Direcţia datelor)
Direcţia traficului de date de urmărit. Direcţia poate fi doar trafic outbound (*SND), doar trafic inbound (*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 îmbrobodeşte de la început. Cele mai vechi înregistrări de urmărire scrise peste cele noi după cum sunt colectate.

A doua valoare *STOPTRC lasă urmărirea oprită când buffer-ul de urmărire, specificat în parametrul MAXSTG, este plin de înregistrări de urmărire. Ca o regulă generală, mereu să definiţi dimensiunea buffer-ului astfel încât să fie suficient de mare ca să reţină toate înregistrările de urmărire. Dacă urmărirea face wrap, aţi putea pierde informaţii importante de urmărire. Dacă experimentaţi o problemă de intermitenţă înaltă, definiţi buffer-ul de urmărire să fie destul de mare astfel ca o derulare a buffer-ului să nu abandoneze informaţii importante.

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

TEXT (Descriere urmărire)
Furnizează o descriere cu sens a urmăririi.

Oprirea urmăririi de comunicaţii

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

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

Comanda are doi parametrii:

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

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

Tipărirea datelor de urmărire

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

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

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

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

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

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

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

TCPIPADR (Formatul de date TCP/IP după adresă)
Acest parametru conţine două elemente. Dacă specificaţi 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 doriţi; de exemplu, cereri ARP (Address Resolution Protocol), specificaţi *NO; altfel s-ar putea să fiţi copleşit de mesaje de broadcast.

Operaţii înrudite

“Iniţiere în depanarea VPN” la pagina 59
Finalizaţi această operaţie pentru a învăţa diversele metode pentru a determina orice probleme VPN din sistemul dumneavoastră.

Informaţii înrudite pentru VPN

Publicaţiile IBM Redbooks şi siturile web conţin informaţii înrudite cu colecţia de subiecte Reţea privată virtuală. Puteţi vizualiza sau tipări oricare dintre aceste fişiere PDF.

IBM Redbooks

- IBM System i Security Guide pentru IBM i5/OS Versiunea 5 Ediţia 4
- AS/400 Internet Security: Implementing AS/400 Virtual Private Networks
- AS/400 Internet Security Scenarios: A Practical Approach
- OS/400 V5R2 Virtual Private Networks: Remote Access to the IBM eServer iSeries Server with Windows 2000 VPN Clients

Situri web

- TCP/IP for i5/OS: Virtual Private Networking
- TCP/IP for i5/OS: RFC Documents

Anexa. Observaţii

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation

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

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

Programul cu licenţă descris în acest document şi în toate produsele cu licenţă disponibile pentru acesta sunt furnizate de către IBM sub termenii Contractului IBM cu Clientul, Contractului IBM de licenţa internaţională a programului, Contractului IBM de licenţă pentru cod maşină sau orice contract echivalent între noi.

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

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

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

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

LICENŢĂ DE COPYRIGHT:

Aceste informaţii cuprind exemple de programe de aplicaţie în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteţi copia, modifica şi distribui aceste programe-eşantion în orice formă fără necesitatea unei plăţi către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicaţie în concordanţă cu interfaţa de programare a aplicaţiei pentru platforma de operare pentru care sunt scrise programele-eşantion. Aceste exemple nu au fost testate complet în toate condiţiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcţionale.

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

© (numele companiei dumneavoastră) (anul). Porţiuni din acest cod sunt derivate din Programe eşantion ale IBM Corp.
© Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vedeţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Informaţii despre interfaţa de programare

Această publicaţie Reţea virtuală privată documentează anumite Interfeţe de programare care permit clientului să scrie programe pentru a obţine servicii IBM i5/OS.

Mărci comerciale

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

Abordare
AS/400
  Echilibrare
eServer
 i5/OS
 IBM
 iSeries
 OS/400
 SAA
 System i

Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt fie mărci comerciale înregistrate fie mărci comerciale ale Adobe Systems Incorporated în Statele Unite, şi/sau alte ţări.

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

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

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţină în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.