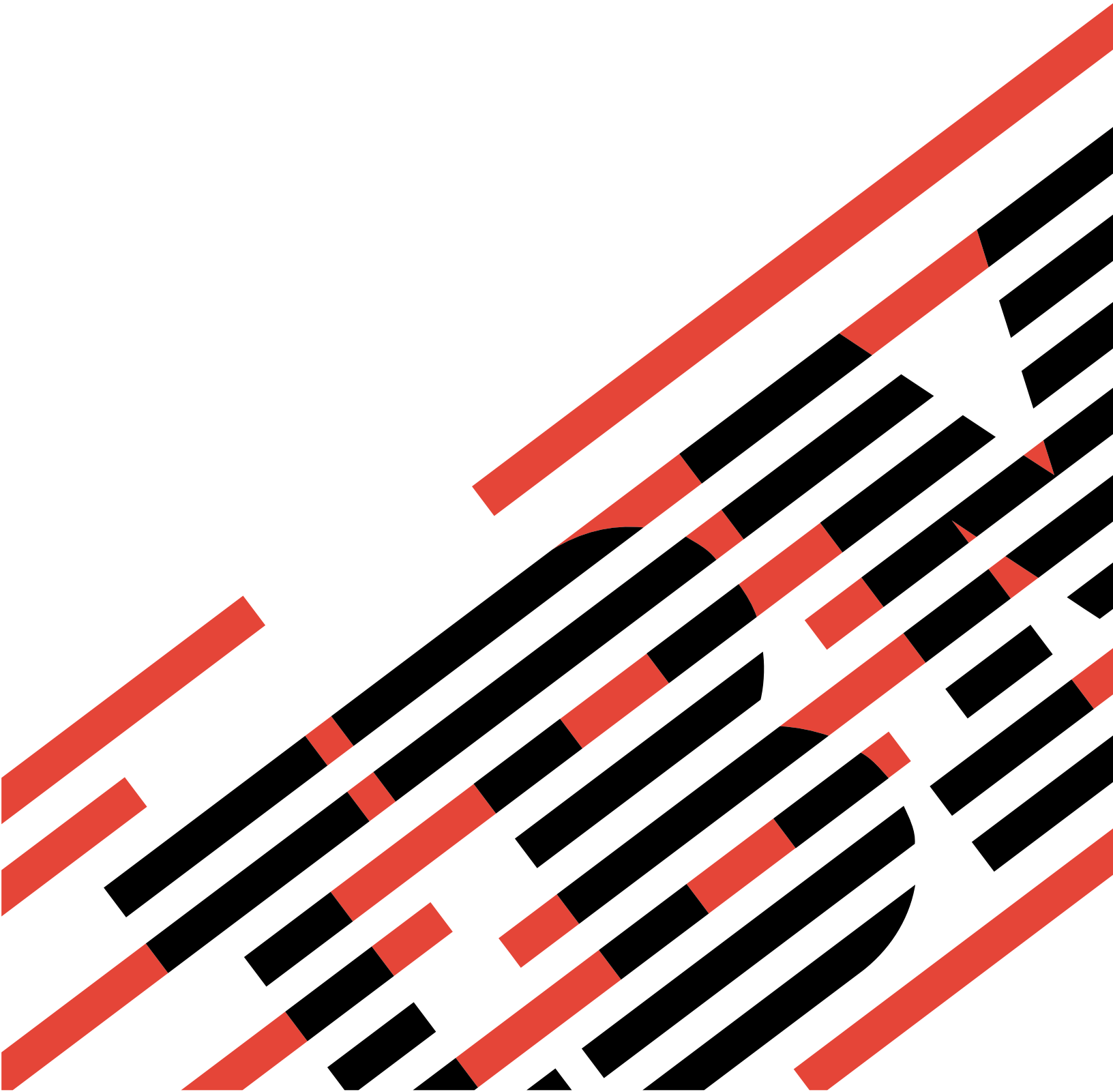
IBM

eserver

iSeries

Virtuális magánhálózatok



IBM

@server

iSeries

Virtuális magánhálózatok

Tartalom

Virtuális magánhálózatok

A virtuális magánhálózatok (VPN) lehetővé teszik a vállalatok számára a belső intranet kiterjesztését a nyilvános hálózatok, például az Internet meglévő infrastruktúrájának felhasználásával. Virtuális magánhálózatokkal felügyelhető a hálózati forgalom, emellett további biztonsági szolgáltatásokat is nyújtanak, például a hitelesítést és az adatok bizalmasságát.

Az OS/400 VPN az OS/400 grafikus felhasználói felületének, az iSeries navigátornak egyik választhatóan telepíthető összetevője. Lehetővé teszi biztonságos útvonalak létrehozását hosztok és átjárók tetszőleges kombinációja között. Az OS/400 VPN a kapcsolat két végpontja között forgalmazott adatok biztonságának érdekében hitelesítési módszereket, titkosítási algoritmusokat és további funkciókat biztosít.

A VPN a TCP/IP rétegekre osztott kommunikációs verem modelljének hálózati rétegén fut. Pontosabban a VPN az IP biztonsági architektúra (IPSec) keretrendszerét használja. Az IPSec alapvető biztonsági funkciókat nyújt az Interneten, emellett rugalmas építőelemeket biztosít hatékony és biztonságos virtuális magánhálózatok létrehozásához.

A VPN funkció támogatja a 2. szintű alagútkezelési protokollt (L2TP) alkalmazó VPN megoldásokat is. A virtuális vonalaknak is nevezett L2TP kapcsolatok költséghatékony hozzáférést biztosítanak a távoli felhasználók számára azáltal, hogy lehetővé teszik a vállalati hálózat szervereinek a távoli felhasználókhoz hozzárendelt IP címek kezelését. Ezen kívül az L2TP kapcsolatok IPSec védelem használata esetén biztonságos hozzáférést nyújtanak a rendszerhez vagy hálózathoz.

Fontos megérteni, hogy a VPN a teljes hálózatra hatással van. A gondos tervezés és megvalósítás a siker kulcsfontosságú része. A virtuális magánhálózatok működésének megértéséhez és felhasználási lehetőségeik megismeréséhez nézze meg a következő témaköröket:

A V5R2 kiadás újdonságai
Ez a témakör írja le a jelenlegi kiadás fontosabb változásait és újdonságait.

A témakör nyomtatása
Ha a kiadványt nyomtatott formában kívánja elolvasni, akkor ebből a témakörből ismerheti meg a nyomtatásra vonatkozó útmutatásokat.

VPN példahelyzetek
A példahelyzetek áttekintésével megismerheti a virtuális magánhálózatok alapvető típusait, illetve a beállításukhoz szükséges lépéseket.

VPN alapelvek
Az információk alkalmazásához fontos, hogy legalább alapszintű ismeretekkel rendelkezzen a virtuális magánhálózatok által alkalmazott technológiákról. Ez a témakör írja le a VPN protokolljaira vonatkozó koncepcionális információkat.

VPN tervezés
A VPN sikeres használatba vételének első lépése a tervezés. Ez a témakör nyújt információkat a korábbi kiadásokról végzett áttérésről, a beállítási követelményekről, illetve itt találja a tervezési tanácsadót is, amely a megadott meghatározásoknak megfelelő tervezési munkalap előállításával segíti munkáját.

VPN beállítása
A VPN megtervezése után megkezdhető a beállítás folyamata. Ez a témakör a VPN lehetőségeit, és ezek megvalósításának módját írja le.

VPN kezelése
Ez a témakör írja le az aktív VPN kapcsolatokon végrehajtható különféle feladatokat, például a kapcsolatok módosítását, megfigyelését és törlését.

VPN hibaelhárítás
Ebben a témakörben talál információkat a problémás VPN kapcsolatok hibaelhárításához.

VPN kapcsolódó információk
Ez a témakör sorolja fel a virtuális magánhálózatokhoz kapcsolódó információkra vonatkozó további kiadványokat és webes hivatkozásokat.

A V5R2 kiadás újdonságai

A V5R2 kiadásban a virtuális magánhálózatok terén történt lényeges továbbfejlesztések a következők:

- NAT-kompatibilis IPSec, más néven UDP beágyazás, amely az IP biztonsági protokoll és a hálózati cím fordítás (NAT) technológiák közötti különféle kompatibilitási problémákat hivatott kiküszöbölni. Az UDP beágyazás lehetővé teszi az iSeries szervernek a NAT funkciót használó tűzfalak mögötti működést. Az OS/400 VPN korábbi kiadásaitól eltérően a VPN kapcsolatok kialakításához az iSeries szervert most már nem kell peremhálózatra helyezni vagy nyilvános címmel ellátni.
- Dinamikus stratégia szűrők. A jelenlegi kiadástól lehetőség van stratégia szűrőszabályok nélküli VPN kapcsolatok létrehozására. A kapcsolat szűrőinek dinamikus kezelését a rendszer végzi, ami annyit jelent, hogy VPN kapcsolatok létrehozásához nem kell csomagszabályokat beállítania.
- Stratégia szűrők átvétele varázsló. Ha frissítette a rendszert a V4R4 vagy V4R5 kiadásról, és használni kívánja a frissítés előtti szabályokat, akkor a Stratégia szabályok átvétele varázsló segítségével távolíthatja el a létrehozott csomagszabály fájlokból a stratégia szűrőket. A varázsló beilleszti az ezekkel egyenértékű stratégia szűrőket a VPN által előállított stratégia szűrők közé. Ez biztosítja a régi és az új stratégia szűrőknek a tervezett együttműködését.
- Továbbfejlesztett titkosítási szabvány (AES) algoritmus. Az OS/400 VPN támogatja az AES titkosítási algoritmust.

A VPN témakör változásai a V5R2 kiadásban:

- További példahelyzetek a VPN szerepéről a vállalati konfigurációkban.
- A frissített VPN tervezési tanácsadó segít az adott üzleti igénynek megfelelő VPN típusának meghatározásában. A tanácsadó emellett a VPN beállításához is segítséget nyújt.

A kiadás további újdonságairól vagy változásairól a Jegyzék a felhasználóknak című témakörben olvashat.

VPN példahelyzetek

Az alábbi példahelyzetek segítségével megismerheti az alábbi alapvető kapcsolattípusok technikai és konfigurációs részleteit:

- **VPN példahelyzet - Telephely kapcsolat**
  Ebben a példahelyzetben a vállalat VPN kialakítását tervezi két távoli részleg között, amelyben két iSeries szerver VPN átjáró lesz.
- **VPN példahelyzet - Üzleti partnerek közötti kapcsolat**
  Ebben a példahelyzetben a vállalat a gyártási részleg egyik kliens munkaállomása és egy üzleti partner szállítási részlegének egyik munkaállomása között alakít egy virtuális magánhálózatot.
- **VPN példahelyzet - L2TP önkéntes alagút védelme IPSec megoldással**
  Ebben a példahelyzetben egy telephely valamelyik hosztjának és a központi iroda hálózatának összekötésére kerül sor IPSec védelemmel ellátott L2TP alagút felhasználásával. A telephely dinamikusan hozzárendelt IP címmel rendelkezik, míg a központi irodának statikus, nyilvánosan továbbítható IP címe van.

- **VPN példahelyzet - Hálózati cím fordítás használata VPN kapcsolatban**
  Ebben a példahelyzetben a vállalat érzékeny adatokat kíván cserélni az egyik üzleti partnerrel az OS/400 VPN szolgáltatásának felhasználásával. A belső hálózat felépítésének eltitkolása érdekében a vállalat VPN NAT használatával elrejti az alkalmazásokat kiszolgáló iSeries szerver IP címét.

További VPN példahelyzetek
További VPN példahelyzeteket a virtuális magánhálózatokkal kapcsolatos alábbi információforrásokban találhat:

- **QoS példahelyzet: Biztonságos és megjósolható eredmények (VPN és QoS)**
  A virtuális magánhálózatban létrehozhatók Szolgáltatási minőség (QoS) irányelvek. Ez a példa mutatja be a két szolgáltatás együttes használatát.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM iSeries Server with Windows 2000 VPN Clients, REDP0153**
  Ez az IBM kiadvány lépésenként megadott útmutatásokat tartalmaz a V5R1 kiadású iSeries szerverek és Windows 2000 kliensek közötti VPN alagutak kialakításához a Windows 2000 saját L2TP és IPSec támogatásának felhasználásával.

- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**
  Ez a kiadvány a VPN alapelveket mutatja be, emellett leírja ezek megvalósítását az IPSec és L2TP protokoll felhasználásával az OS/400 rendszereken.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**
  Ez a kiadvány az AS/400 rendszerek valamennyi hálózati biztonsági szolgáltatását bemutatja, köztük az IP szűrést, a hálózati cím fordítást, a virtuális magánhálózatokat, a HTTP proxy szervereket, az SSL protokollt, valamint a DNS, levéltovábbítási, megfigyelési és naplózási szolgáltatásokat. Az egyes szolgáltatások használatára gyakorlati példákat is bemutat.

VPN példahelyzet - Telephely kapcsolat

Tegyük fel, hogy a vállalat minimálisra kívánja csökkenteni a telephelyek közötti kommunikáció költségeit. Korábban a kommunikációt kerettovábbító vagy bérelt vonalak biztosították, de felmerült az igény egy kevésbé költséges, biztonságosabb és globálisan elérhető átviteli megoldás iránt. Az Internet lehetőségeinek kihasználásával az igény egyszerűen kielégíthető egy virtuális magánhálózat létrehozásával.

A vállalatnak és a telephelynek is szüksége van a VPN által nyújtott biztonságra az Internetes továbbításhoz, a megfelelő intranetekben azonban nincs ilyen biztonsági igény. Mivel az intranetek megbízhatónak feltételezhetők, a legjobb megoldás egy átjáró-átjáró VPN lenne. Ebben az esetben mindkét átjáró közvetlenül csatlakozik a köztes hálózathoz. Más szavakkal ezek *határ-* vagy *perem*rendszerek, amelyeket nem védenek tűzfalak. A példa hasznos bevezetést nyújt az alapszintű VPN konfigurációk beállításához szükséges lépések megismeréséhez. A példahelyzetben az *internet* kifejezés a két VPN átjáró közötti hálózatot jelenti, amely lehet a vállalat saját hálózata, de lehet az Internet is.

> **Fontos megjegyzés:**
> A példahelyzetben az iSeries szerver közvetlenül az Internethez csatlakozik. A tűzfal hiánya a példahelyzet egyszerűsítését szolgálja. Nem kívánjuk sugallni, hogy a tűzfal nem szükséges. Valójában minden egyes Internet csatlakozáskor végig kell gondolni az ebből származó biztonsági kockázatok lehetőségeit. Az ilyen kockázatok csökkentésére használható különféle módszerekről az AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00 című kiadványból tájékozódhat.

Előnyök

A példahelyzet a következő előnyöket biztosítja:

- Az Internet vagy egy meglévő intranet használata csökkenti a távoli alhálózatokat összekötő saját vonalakból adódó költségeket.
- Az Internet vagy egy meglévő intranet használata csökkenti a saját vonalak és az ezekhez csatlakozó berendezések szerelésével és karbantartásával kapcsolatos terhelést.
- Az Internet használatával a távoli helyek a világon szinte bárhova csatlakozhatnak.
- A VPN lehetővé teszi a felhasználóknak, hogy a kapcsolat másik oldalán található szervereket és erőforrásokat úgy használják, mintha az összeköttetést bérelt vonal vagy nagy kiterjedésű hálózat (WAN) biztosítaná.
- A helyszínek között forgalmazott információk biztonságát ipari szabvány titkosítási és hitelesítési módszerek biztosítják.
- A titkosítási kulcsok rendszeres és dinamikus cseréje minimálisra csökkenti annak esélyét, hogy a kulcsokat visszafejtsék, és segítségükkel hozzáférjenek a bizalmas információkhoz.
- Minden távoli alhálózat saját IP címeket használ, így nincs szükség minden egyes kliens számára értékes nyilvános IP cím igénylésére.

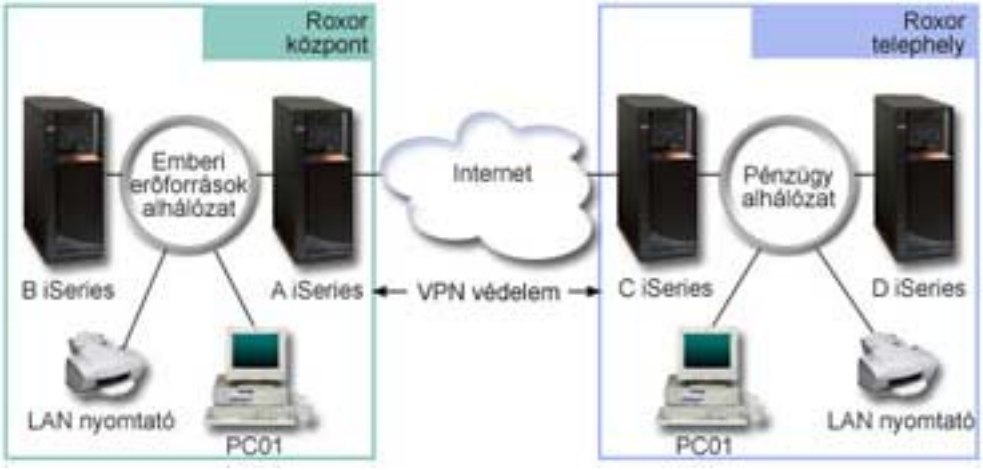
Célok

Ebben a példahelyzetben a Roxor Kft. VPN kialakítását tervezi az Emberi erőforrások és a Pénzügy részleg között két iSeries szerveren keresztül. Mindkét szerver VPN átjáróként fog működni. A VPN konfigurációk szóhasználatában az átjárók végzik a kulcskezelést, és alkalmazzák az IPSec protokollt az alagútón átküldött adatokra. Az átjárók nem a kapcsolat adatvégpontjai.

A példahelyzet céljai a következők:
- A virtuális magánhálózatnak meg kell védenie az Emberi erőforrások részleg alhálózata és a Pénzügyi részleg alhálózata között forgalmazott adatokat.
- Az adatforgalom nem igényli a VPN védelmét, miután eléri valamelyik részleg alhálózatát.
- Mindkét hálózat minden kliense és hosztja teljes körű hozzáféréssel bír a másik hálózathoz, és annak minden alkalmazásához.
- Az átjáró szerverek kommunikálhatnak egymással, és elérhetik a másikon futó alkalmazásokat.

Részletek

A Roxor hálózatának jellemzőit az alábbi ábra szemlélteti.



Emberi erőforrások részleg
- Az A nevű iSeries szerveren az OS/400 V5R2 kiadása fut, ez az Emberi erőforrások részleg VPN átjárója.

- Az alhálózat címe 10.6.0.0, a használt alhálózati maszk 255.255.0.0. Ez az alhálózat képviseli a Roxor budapesti irodájában található VPN alagút adatvégpontját.
- Az A iSeries szerver a 204.146.18.227 IP címmel csatlakozik az Internetre. Ez a kapcsolati végpont. Ez azt jelenti, hogy az A iSeries végzi a kulcskezelést, és alkalmazza az IPSec protokollt a kimenő és bejövő IP adatcsomagokra.
- Az A iSeries a saját alhálózatához a 10.6.11.1 IP címmel csatlakozik.
- A B iSeries az Emberi erőforrások részleg termelési szervere, amelyen szabványos TCP/IP alkalmazások futnak.

Pénzügyi részleg

- A C nevű iSeries szerveren az OS/400 V5R2 kiadása fut, ez a Pénzügyi részleg VPN átjárója.
- Az alhálózat címe 10.196.8.0, a használt alhálózati maszk 255.255.255.0. Ez az alhálózat képviseli a Roxor szegedi irodájában található VPN alagút adatvégpontját.
- A C iSeries szerver a 208.222.150.250 IP címmel csatlakozik az Internetre. Ez a kapcsolati végpont. Ez azt jelenti, hogy a C iSeries végzi a kulcskezelést, és alkalmazza az IPSec protokollt a kimenő és bejövő IP adatcsomagokra.
- A C iSeries a saját alhálózatához a 10.196.8.5 IP címmel csatlakozik.

Konfigurációs feladatok

A példahelyzetben felvázolt telephely kapcsolatának beállításához a következő feladatokat kell elvégezni:

1. A TCP/IP útválasztás ellenőrzésével győződjön meg róla, hogy a két átjáró szerver képes kommunikálni egymással az Interneten keresztül. Ez biztosítja, hogy az egyes alhálózatok hosztjai a megfelelő átjárón keresztül csatlakozni tudnak a másik alhálózathoz.
   Megjegyzés: Az útvonalkezelés meghaladja ezen témakör kereteit. Ha ezzel kapcsolatban lennének kérdései, akkor nézze meg az Információs központ TCP/IP útvonalkezelés és terheléskiegyenlítés című témakörét.
2. Töltse ki (Lásd: 5) mindkét rendszer tervezési munkalapját és ellenőrzőlistáit.
3. Állítsa be (Lásd: 6) a VPN-t az Emberi erőforrások részleg VPN átjáróján (A jelű iSeries).
4. Állítsa be (Lásd: 7) a VPN-t a Pénzügyi részleg VPN átjáróján (B jelű iSeries).
5. Győződjön meg róla, hogy a VPN szerverek elindultak (Lásd: 7).
6. Tesztelje (Lásd: 8) a kommunikációt a két távoli alhálózat között.

Konfiguráció részletei

Az első lépés végrehajtása, vagyis a TCP/IP útvonalkezelés működésének és az átjáró szerverek kommunikációjának ellenőrzése után készen áll a VPN beállításának megkezdésére.

2. lépés - Tervezési munkalapok kitöltése

A következő tervezési ellenőrzőlisták a VPN beállításának megkezdése előtt összegyűjtendő információkat szemléltetik. Az előfeltételek ellenőrzőlistáján valamennyi kérdés mellett Igen válasznak kell állnia ahhoz, hogy megkezdhesse a VPN beállítását.

Megjegyzés: A munkalapok az A jelű iSeries szerverre vonatkoznak, a folyamat az IP címek megfelelő behelyettesítésével alkalmazható a C jelű iSeries szerverre.

Előfeltétel ellenőrzőlista	Válaszok
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	Igen
A Digitális igazolás kezelő (5722-SS1, 34. opció) telepítve van?	Igen

Van telepített Cryptographic Access Provider (5722-AC2 vagy AC3) termék?	Igen
Telepítve van az iSeries Access for Windows (5722-XE1) termék?	Igen
Telepítve van az iSeries navigátor?	Igen
Telepítve van az iSeries navigátor Hálózat részösszetevője?	Igen
Telepítve van a TCP/IP Connectivity Utilities for OS/400 (5722-TC1) termék?	Igen
Beállította a Szerver biztonsági adatok megtartása (QRETSVRSEC *SEC) rendszerváltozót 1-re?	Igen
Be van állítva a TCP/IP az iSeries szerveren (beleértve az IP csatolókat, útvonalakat, a helyi hosztnevet és a helyi tartománynevet)?	Igen
A szokásos TCP/IP kommunikáció működik a szükséges végpontok között?	Igen
Alkalmazta a legújabb ideiglenes program javításokat (PTF)?	Igen
Ha a VPN alagút forgalma tűzfalakon vagy IP csomagszűrést megvalósító útválasztókon halad át, akkor támogatja a tűzfal vagy útválasztó az AH és ESP protokollokat?	Igen
A tűzfalak vagy útválasztók be vannak állítva az IKE (UDP 500-as port), AH és ESP protokollokhoz?	Igen
A tűzfalakon be van állítva az IP továbbítás?	Igen

A VPN beállításához szükséges információk	**Válaszok**
Milyen típusú kapcsolatot hoz létre?	átjáró-átjáró
Mi lesz a dinamikus kulcsú csoport neve?	HRgw2FINgw
Milyen biztonságot és rendszerteljesítményt követel meg a kulcsok védelméhez?	kiegyensúlyozott
Igazolásokat használ a kapcsolat hitelesítéséhez? Ha nem, akkor mi az előzetesen megosztott kulcs?	Nem nagyon titkos
Mi a helyi kulcsszerver azonosítója?	IP cím: 204.146.18.227
Mi a helyi adatvégpont azonosítója?	Alhálózat: 10.6.0.0 Maszk: 255.255.0.0
Mi a távoli kulcsszerver azonosítója?	IP cím: 208.222.150.250
Mi a távoli adatvégpont azonosítója?	Alhálózat: 10.196.8.0 Maszk: 255.255.255.0
Milyen portokat és protokollokat kíván átengedni a kapcsolaton?	Bármilyen
Milyen biztonságot és rendszerteljesítményt követel meg az adatok védelméhez?	kiegyensúlyozott
Milyen csatolókra vonatkozik a kapcsolat?	TRLINE

3. lépés - A VPN beállítása az A jelű iSeries szerveren

A munkalapokon megadott információk segítségével állítsa be a VPN-t az A jelű iSeries szerveren az alábbiak szerint:

1. Az iSeries navigátorban bontsa ki az A jelű iSeries szerver **—> Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Új kapcsolat** menüpontját az Új kapcsolat varázsló indításához.
3. Az **Üdvözlet** lapon tekintse át a varázsló által létrehozott objektumokra vonatkozó információkat.
4. A **Tovább** gombbal lépjen tovább a **Kapcsolat neve** lapra.
5. A **Név** mezőben adja meg a HRgw2FINgw értéket.
6. Adja meg a kapcsolati csoport leírását. (nem kötelező)

7. A **Tovább** gombbal lépjen tovább a **Kapcsolati példahelyzet** lapra.
8. Válassza ki az **Átjáró csatlakoztatása egy másik átjáróhoz** lehetőséget.
9. A **Tovább** gombbal lépjen tovább az **Internet kulcscsere stratégia** lapra.
10. Válassza ki az **Új stratégia létrehozása** lehetőséget, majd válassza ki a **Kiegyensúlyozott biztonság és teljesítmény** beállítást.
11. A **Tovább** gombbal lépjen tovább a **Helyi kapcsolati végpont igazolása** lapra.
12. A **Nem** választásával adja meg, hogy a kapcsolat hitelesítéséhez nem igazolásokat fog használni.
13. A **Tovább** gombbal lépjen tovább a **Helyi kulcsszerver** lapra.
14. Az **Azonosító típusa** mezőben válassza ki az **IPv4 cím** értéket.
15. Az **IP cím** mezőbe írja be a 204.146.18.227 címet.
16. A **Tovább** gombbal lépjen tovább a **Távoli kulcsszerver** lapra.
17. Az **Azonosító típusa** mezőben válassza ki az **IPv4 cím** értéket.
18. Az **Azonosító** mezőben adja meg a 208.222.150.250 címet.
19. Az **Előzetesen megosztott kulcs** mezőbe írja be a nagyon titkos szót.
20. A **Tovább** gombbal lépjen tovább a **Helyi adatvégpont** lapra.
21. Az **Azonosító típusa** mezőben válassza ki az **IPv4 alhálózat** értéket.
22. Az **Azonosító** mezőben adja meg a 10.6.0.0 címet.
23. Az **Alhálózati maszk** mezőben adja meg a 255.255.0.0 maszkot.
24. A **Tovább** gombbal lépjen tovább a **Távoli adatvégpont** lapra.
25. Az **Azonosító típusa** mezőben válassza ki az **IPv4 alhálózat** értéket.
26. Az **Azonosító** mezőben adja meg a 10.196.8.0 címet.
27. Az **Alhálózati maszk** mezőben adja meg a 255.255.255.0 maszkot.
28. A **Tovább** gombbal lépjen tovább az **Adat szolgáltatások** lapra.
29. Fogadja el az alapértelmezett értékeket, majd a **Tovább** gombbal lépjen tovább az **Adat stratégia** lapra.
30. Válassza ki az **Új stratégia létrehozása** lehetőséget, majd válassza ki a **Kiegyensúlyozott biztonság és teljesítmény** beállítást. Válassza ki az **RC4 titkosítás használata** beállítást.
31. A **Tovább** gombbal lépjen tovább a **Megfelelő csatolók** lapra.
32. A **Vonal** táblázatból válassza ki a **TRLINE** vonalat.
33. A **Tovább** gombbal lépjen tovább az **Összegzés** lapra. Tekintse át a varázsló által létrehozott objektumokat, és győződjön meg róla, hogy helyesek.
34. A konfiguráció befejezéséhez kattintson a **Befejezés** gombra.
35. A **Stratégia szűrők aktiválása** párbeszédablak megjelenésekor válassza az **Igen, előállított stratégia szűrők aktiválása** lehetőséget, majd válassza ki a **Minden más forgalom engedélyezése** beállítást. A konfiguráció befejezéséhez kattintson az **OK** gombra. Ha erre felszólítást kap, akkor adja meg a szabályok aktiválását minden csatolón.

Az A jelű iSeries szerveren befejeződött a VPN beállítása. A következő lépés a Pénzügyi részleg VPN átjárójának (C jelű iSeries) beállítása.

4. lépés - VPN beállítása a C jelű iSeries szerveren

Kövesse az A jelű iSeries beállításának lépéseit az IP címek értelemszerű cseréjével. Segítségként használja a tervezési munkalapokat. A Pénzügyi részlegen található VPN átjáró konfigurálásának befejezése után a kapcsolatok állapota *kérésre* lesz, ami annyit tesz, hogy a kapcsolat akkor indul el, ha a VPN által védendő IP adatcsomagok küldésére kerül sor. A következő lépés a VPN szerverek indítása, ha erre még nem került volna sor.

5. lépés - VPN szerverek indítása

A VPN szerverek indításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Szerver —> Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Indítás** menüpontját.

6. lépés - Kapcsolat tesztelése

A beállítások elvégzése és a VPN szerverek sikeres elindítása után a kapcsolat tesztelésével győződjön meg róla, hogy az alhálózatok képesek egymással kommunikálni. Ehhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries —> Hálózat** elemet.
2. Kattintson a jobb egérgombbal a **TCP/IP konfiguráció** elemre, majd válassza az előugró menü **Segédprogramok —> Ping** menüpontját.
3. A **Pingelés az A iSeries szerverről** párbeszédablak **Ping** mezőjében adja meg a C iSeries hosztnevét.
4. Kattintson a **Pingelés** gombra az A és C iSeries szerverek közötti kapcsolat ellenőrzéséhez.
5. Ha befejezte, kattintson az **OK** gombra.

VPN példahelyzet - Üzleti partnerek közötti kapcsolat

Az üzleti partnerekkel, leányvállalatokkal és szállítókkal folytatott biztonságos kommunikációhoz sok vállalat használ kerettovábbító vagy bérelt vonalakat. Ezek a megoldások sajnos gyakran költségesek, és földrajzi korlátai is vannak. A VPN alternatívát nyújt a biztonságos, költséghatékony kommunikációt igénylő vállalatok számára.

Vegyünk példaként egy gyártócéget és egy alkatrész beszállítót. Mivel az alkatrész beszállító számára rendkívül fontos, hogy a gyártó cég által igényelt alkatrészek rendelkezésre álljanak a kért mennyiségben és időpontra, folyamatosan információkkal kell rendelkeznie a gyártó raktárkészletéről és a termelés ütemezéséről. Elképzelhető, hogy ez jelenleg kézi feldolgozással történik, ez azonban időigényes, költséges, és bizonyos esetekben pontatlan is. A beszállító könnyebb, gyorsabb és hatékonyabb utat keres a gyártócéggel folytatott kommunikációhoz. A cserélt információk bizalmas és idő szempontjából kritikus természete miatt a gyártó nem szeretné ezeket sem a webhelyén publikálni, sem havi jelentésben szétküldeni. Az Internet lehetőségeinek kihasználásával mindkét igény egyszerűen kielégíthető egy virtuális magánhálózat létrehozásával.

Célok

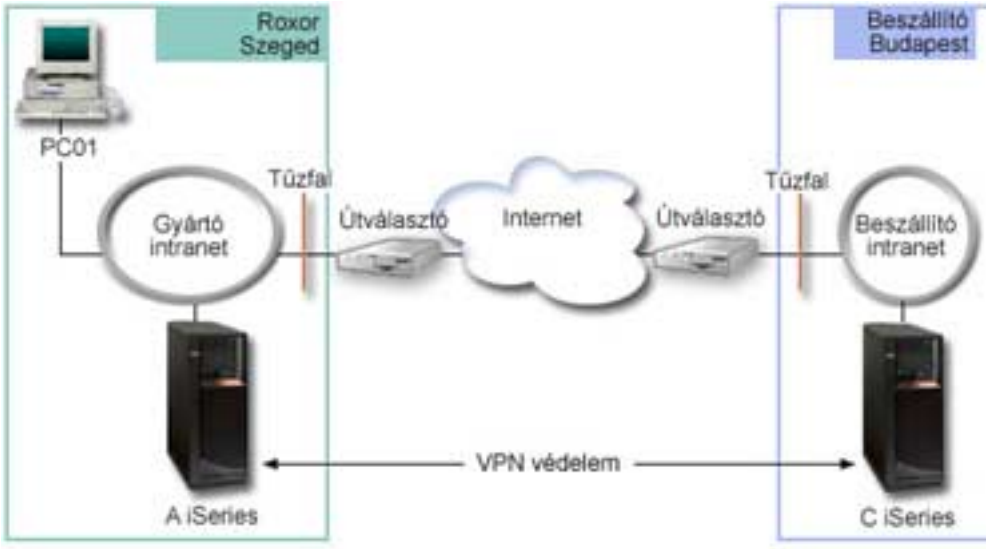
Ebben a példahelyzetben a Roxor Kft. a saját alkatrész részlegének egyik hosztja, illetve az üzleti partner gyártási részlegének egyik hosztja között szeretne virtuális magánhálózatot kialakítani.

Mivel a két vállalat által cserélt információk bizalmasak, ezeket meg kell védeni az Interneten való áthaladás során. Emellett az adatok a vállalati hálózatokon sem küldhetők titkosítatlanul, mivel mindkét hálózat megbízhatatlannak feltételezi a másik hálózatot. Más szavakkal mindkét vállalat végpont-végpont hitelesítést, integritást és titkosítást igényel.

Fontos megjegyzés:
A példahelyzet célja egy egyszerű, hosztok közötti VPN konfiguráció bemutatása. Egy jellemző hálózati környezetekben ezek mellett meg kell fontolni a tűzfalak beállításait, az IP címekre vonatkozó követelményeket és az útválasztást is, hogy csak néhányat említsünk.

Részletek

A Roxor és az üzleti partner hálózatának jellemzőit az alábbi ábra szemlélteti:



A Roxor alkatrész részlegének hálózata

- Az A nevű iSeries szerveren az OS/400 V5R2 kiadása fut.
- Az A iSeries IP címe 10.6.1.1. Ez a kapcsolati végpont és az adatvégpont is egyben. Ez azt jelenti, hogy az A iSeries végzi az IKE egyeztetéseket, és alkalmazza az IPSec protokollt a kimenő és bejövő IP adatcsomagokra, emellett ez a szerver a VPN kapcsolaton átküldött adatok forrása és célja is.
- Az A iSeries a 10.6.0.0 alhálózatban található, amelynek alhálózati maszkja 255.255.0.0.
- Csak az A iSeries kezdeményezheti a kapcsolatot a C iSeries felé.

Üzleti partner gyártási részlegének hálózata

- A C nevű iSeries szerveren az OS/400 V5R2 kiadása fut.
- A C iSeries IP címe 10.196.8.6. Ez a kapcsolati végpont és az adatvégpont is egyben. Ez azt jelenti, hogy az A iSeries végzi az IKE egyeztetéseket, és alkalmazza az IPSec protokollt a kimenő és bejövő IP adatcsomagokra, emellett ez a szerver a VPN kapcsolaton átküldött adatok forrása és célja is.
- A C iSeries a 10.196.8.0 alhálózatban található, amelynek alhálózati maszkja 255.255.255.0.

Konfigurációs feladatok

A példahelyzetben felvázolt üzleti partnerek közötti kapcsolat beállításához a következő feladatokat kell elvégezni:

1. A TCP/IP útválasztás ellenőrzésével győződjön meg róla, hogy az A és C iSeries képes kommunikálni egymással az Interneten keresztül. Ez biztosítja, hogy az egyes alhálózatok hosztjai a megfelelő átjárón keresztül csatlakozni tudnak a másik alhálózathoz. Figyelni kell arra, hogy a példahelyzetben át kell gondolni a saját címek továbbítását, amely elképzelhető, hogy még nem merült fel.

   Megjegyzés: Az útvonalkezelés meghaladja ezen témakör kereteit. Ha ezzel kapcsolatban lennének kérdései, akkor nézze meg az Információs központ TCP/IP útvonalkezelés és terheléskiegyenlítés című témakörét.
2. Töltse ki (Lásd: 10) mindkét rendszer tervezési munkalapját és ellenőrzőlistáit.
3. Állítsa be (Lásd: 11) a VPN-t a Roxor Kft. alkatrész részlegének A jelű iSeries szerverén.
4. Állítsa be (Lásd: 12) a VPN-t az üzleti partner gyártási részlegének C jelű iSeries szerverén.
5. Aktiválja (Lásd: 12) a szűrőszabályokat mindkét szerveren.
6. Indítsa el (Lásd: 12) a kapcsolatot az A iSeries szerverről.
7. Tesztelje (Lásd: 12) a kommunikációt a két távoli alhálózat között.

Konfiguráció részletei

Az első lépés végrehajtása, vagyis a TCP/IP útvonalkezelés működésének és a szerverek kommunikációjának ellenőrzése után készen áll a VPN beállításának megkezdésére.

2. lépés - Tervezési munkalapok kitöltése

A következő tervezési ellenőrzőlisták a VPN beállításának megkezdése előtt összegyűjtendő információkat szemléltetik. Az előfeltételek ellenőrzőlistáján valamennyi kérdés mellett Igen válasznak kell állnia ahhoz, hogy megkezdhesse a VPN beállítását.

Megjegyzés: A munkalapok az A jelű iSeries szerverre vonatkoznak, a folyamat az IP címek megfelelő behelyettesítésével alkalmazható a C jelű iSeries szerverre.

Előfeltétel ellenőrzőlista	**Válaszok**
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	Igen
A Digitális igazolás kezelő (5722-SS1, 34. opció) telepítve van?	Igen
Van telepített Cryptographic Access Provider (5722-AC2 vagy AC3) termék?	Igen
Telepítve van az iSeries Access for Windows (5722-XE1) termék?	Igen
Telepítve van az iSeries navigátor?	Igen
Telepítve van az iSeries navigátor Hálózat részösszetevője?	Igen
Telepítve van a TCP/IP Connectivity Utilities for OS/400 (5722-TC1) termék?	Igen
Beállította a Szerver biztonsági adatok megtartása (QRETSVRSEC *SEC) rendszerváltozót 1-re?	Igen
Be van állítva a TCP/IP az iSeries szerveren (beleértve az IP csatolókat, útvonalakat, a helyi hosztnevet és a helyi tartománynevet)?	Igen
A szokásos TCP/IP kommunikáció működik a szükséges végpontok között?	Igen
Alkalmazta a legújabb ideiglenes program javításokat (PTF)?	Igen
Ha a VPN alagút forgalma tűzfalakon vagy IP csomagszűrést megvalósító útválasztókon halad át, akkor támogatja a tűzfal vagy útválasztó az AH és ESP protokollokat?	Igen
A tűzfalak vagy útválasztók be vannak állítva az IKE (UDP 500-as port), AH és ESP protokollokhoz?	Igen
A tűzfalakon be van állítva az IP továbbítás?	Igen

A VPN beállításához szükséges információk	**Válaszok**
Milyen típusú kapcsolatot hoz létre?	hoszt-hoszt
Mi lesz a dinamikus kulcsú csoport neve?	MyCo2TheirCo
Milyen biztonságot és rendszerteljesítményt követel meg a kulcsok védelméhez?	legnagyobb biztonság
Igazolásokat használ a kapcsolat hitelesítéséhez? Ha nem, akkor mi az előzetesen megosztott kulcs?	Igen
Mi a helyi kulcsszerver azonosítója?	IP cím: 10.6.1.1
Mi a helyi adatvégpont azonosítója?	IP cím: 10.6.1.1
Mi a távoli kulcsszerver azonosítója?	IP cím: 10.196.8.6
Mi a távoli adatvégpont azonosítója?	IP cím: 10.196.8.6
Milyen portokat és protokollokat kíván átengedni a kapcsolaton?	Bármilyen
Milyen biztonságot és rendszerteljesítményt követel meg az adatok védelméhez?	legnagyobb biztonság
Milyen csatolókra vonatkozik a kapcsolat?	TRLINE

3. lépés - A VPN beállítása az A jelű iSeries szerveren

A munkalapokon megadott információk segítségével állítsa be a VPN-t az A jelű iSeries szerveren az alábbiak szerint:

1. Az iSeries navigátorban bontsa ki a szerver **—> Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Új kapcsolat** menüpontját a Kapcsolat varázsló indításához.
3. Az **Üdvözlet** lapon tekintse át a varázsló által létrehozott objektumokra vonatkozó információkat.
4. A **Tovább** gombbal lépjen tovább a **Kapcsolat neve** lapra.
5. A **Név** mezőben adja meg a MyCo2TheirCo értéket.
6. Adja meg a kapcsolati csoport leírását. (nem kötelező)
7. A **Tovább** gombbal lépjen tovább a **Kapcsolati példahelyzet** lapra.
8. Válassza ki az **Hoszt csatlakoztatása hoszthoz** lehetőséget.
9. A **Tovább** gombbal lépjen tovább az **Internet kulcscsere stratégia** lapra.
10. Válassza ki az **Új stratégia létrehozása** lehetőséget, majd válassza ki a **Legnagyobb biztonság, legkisebb teljesítmény** beállítást.
11. A **Tovább** gombbal lépjen tovább a **Helyi kapcsolati végpont igazolása** lapra.
12. Az **Igen** választásával adja meg, hogy a kapcsolat hitelesítéséhez igazolásokat fog használni. Ezután válassza ki az A jelű iSeries szervert képviselő igazolást.
    Megjegyzés: Ha a helyi kapcsolati végpont hitelesítéséhez igazolást kíván használni, akkor először létre kell hozni az igazolást a Digitális igazolás kezelőben (DCM).
13. A **Tovább** gombbal lépjen tovább a **Helyi kapcsolati végpont azonosítója** lapra.
14. Azonosítótípusként válassza ki az **IPv4 cím** értéket. A társított IP címnek 10.6.1.1-nek kell lennie. Ne feledje: ez az érték a Digitális igazolás kezelőben létrehozott igazolásban van megadva.
15. A **Tovább** gombbal lépjen tovább a **Távoli kulcsszerver** lapra.
16. Az **Azonosító típusa** mezőben válassza ki az **IPv4 cím** értéket.
17. Az **Azonosító** mezőben adja meg a 10.196.8.6 címet.
18. A **Tovább** gombbal lépjen tovább az **Adat szolgáltatások** lapra.
19. Fogadja el az alapértelmezett értékeket, majd a **Tovább** gombbal lépjen tovább az **Adat stratégia** lapra.
20. Válassza ki az **Új stratégia létrehozása** lehetőséget, majd válassza ki a **Legnagyobb biztonság, legkisebb teljesítmény** beállítást. Válassza ki az **RC4 titkosítás használata** beállítást.
21. A **Tovább** gombbal lépjen tovább a **Megfelelő csatolók** lapra.
22. Válassza ki a **TRLINE** bejegyzést.
23. A **Tovább** gombbal lépjen tovább az **Összegzés** lapra. Tekintse át a varázsló által létrehozott objektumokat, és győződjön meg róla, hogy helyesek.
24. A konfiguráció befejezéséhez kattintson a **Befejezés** gombra.
25. A **Stratégia szűrők aktiválása** párbeszédablak megjelenésekor válassza a **Nem, előállított stratégia szűrők aktiválása később** lehetőséget, majd kattintson az **OK** gombra.

A következő lépés annak meghatározása, hogy csak az A iSeries kezdeményezheti a kapcsolatot. Ezt a varázsló által létrehozott MyCo2TheirCo dinamikus kulcsú csoport tulajdonságainak módosításával érheti el:

1. A VPN felület bal oldali ablakrészében kattintson a **Csoportonként** beállításra. A MyCo2TheirCo új dinamikus kulcsú csoport megjelenik a jobb oldali ablakrészben. Kattintson rá a jobb egérgombbal, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. Kattintson a **Stratégia** lapra, majd válassza ki a **Helyi rendszer kezdeményezheti a kapcsolatot** beállítást.

3. Kattintson az **OK** gombra a változások mentéséhez.

Az A jelű iSeries szerveren befejeződött a VPN beállítása. A következő lépés az üzleti partner gyártási részlegén található C jelű iSeries beállítása.

4. lépés - VPN beállítása a C jelű iSeries szerveren

Kövesse az A jelű iSeries beállításának lépéseit az IP címek értelemszerű cseréjével. Segítségként használja a tervezési munkalapokat. A C jelű iSeries beállításának befejezése után mindkét szerveren aktiválni kell a Kapcsolat varázsló által létrehozott szűrőszabályokat.

5. lépés - Csomagszabályok aktiválása

A varázsló automatikusan létrehozza a kapcsolat megfelelő működéséhez szükséges csomagszabályokat. Ettől függetlenül ezeket aktiválni kell mindkét rendszeren, mielőtt a VPN kapcsolatot el lehetne indítani. Ehhez az A iSeries szerveren tegye a következőket:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries szerver —> Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomagszabályok** elemre, majd válassza az előugró menü **Aktiválás** menüpontját. Megjelenik a Csomagszabályok aktiválása párbeszédablak.
3. Válassza ki, hogy csak a VPN által előállított szabályokat vagy csak a megadott fájlban található szabályokat kívánja-e aktiválni. Megadhatja mindkét típusú szabálykészlet aktiválását is. Az utóbbi választása akkor lehet szükséges, ha rendelkezik különféle PERMIT és DENY szabályokkal, amelyeket a VPN által előállított szabályok mellett szintén érvénybe kíván léptetni a csatolón.
4. Válassza ki a csatolót, amelyen a szabályokat aktiválni kívánja. Ebben az esetben válassza a **Minden csatoló** beállítást.
5. Kattintson a párbeszédablak **OK** gombjára a szabályok ellenőrzéséhez és aktiválásához a kijelölt csatolón vagy csatolókon. Az OK gomb megnyomása után a rendszer ellenőrzi a szabályok szintaxisát, ennek eredményeit pedig a szövegszerkesztő alján található üzenet területre írja. Az adott fájlhoz és sorhoz köthető hibaüzenetek esetén kattintson a jobb egérgombbal a hibára, majd válassza az előugró menü **Ugrás sorra** menüpontját a sor kijelöléséhez.
6. A fenti lépések megismétlésével aktiválja a csomagszabályokat a C iSeries szerveren is.

6. lépés - Kapcsolat indítása

A kapcsolat indításához tegye a következőket az A jelű iSeries szerveren:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries szerver —> Hálózat —> IP stratégiák** elemeket.
2. Ha a VPN szerver nincs elindítva, akkor kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Indítás** menüpontját. Elindul a VPN szerver.
3. Bontsa ki a **Virtuális magánhálózatok —> Védett kapcsolatok** elemet.
4. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
5. Kattintson a jobb egérgombbal a **MyCo2TheirCo** bejegyzésre, majd válassza az előugró menü **Indítás** menüpontját.
6. Válassza a **Nézet** menü **Frissítés** menüpontját. Ha a kapcsolat sikeresen elindult, akkor az állapotnak *Inaktív* helyett *Engedélyezett* állapotban kell lennie. A kapcsolat indítása eltarthat pár percig, ezért időnként frissítse a nézetet, amíg az állapot nem változik meg *Engedélyezettre*.

7. lépés - Kapcsolat tesztelése

A beállítások elvégzése és a kapcsolat sikeres elindítása után az összeköttetés tesztelésével győződjön meg róla, hogy a távoli hosztok képesek egymással kommunikálni. Ehhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries —> Hálózat** elemet.
2. Kattintson a jobb egérgombbal a **TCP/IP konfiguráció** elemre, majd válassza az előugró menü **Segédprogramok —> Ping** menüpontját.
3. A **Pingelés az A iSeries szerverről** párbeszédablak **Ping** mezőjében adja meg a C iSeries hosztnevét.
4. Kattintson a **Pingelés** gombra az A és C iSeries szerverek közötti kapcsolat ellenőrzéséhez.
5. Ha befejezte, kattintson az **OK** gombra.

VPN példahelyzet - L2TP önkéntes alagút védelme IPSec megoldással

Tegyük fel, hogy egy vállalat fiókirodával rendelkezik egy másik városban. A fiókirodának minden munkanapon hozzá kell férnie a vállalati intranet egyik iSeries szerverén tárolt bizalmas információkhoz. A vállalat jelenleg egy költséges bérelt vonalon biztosítja a fiókirodák hozzáférését a vállalati hálózathoz. Bár a vállalatnak továbbra is célja az intranet biztonságos elérésének biztosítása, a bérelt vonal költségvonzatait mindenképpen csökkenteni szeretné. Ezt egy L2TP önkéntes alagúttal lehet megoldani, amely úgy terjeszti ki a vállalati hálózatot, mintha a fiókiroda annak szerves része lenne. Az L2TP alagúton forgalmazott adatokat pedig VPN védi.

Egy L2TP önkéntes alagúttal a fiókiroda közvetlen kapcsolatot épít ki a vállalati hálózat L2TP hálózati szerverével (LNS). Az L2TP összesítő (LAC) funkcionalitást a kliens biztosítja. Az alagút transzparens a távoli kliens Internet szolgáltatója számára, így az Internet szolgáltatónak nem kell támogatnia az L2TP használatot. Az L2TP alapelvekről további információkhoz a 2. szintű alagútkezelési protokoll (L2TP) című témakörből juthat.

> **Fontos megjegyzés:**
> A példahelyzetben az iSeries szerver közvetlenül az Internethez csatlakozik. A tűzfal hiánya a példahelyzet egyszerűsítését szolgálja. Nem kívánjuk sugallni, hogy a tűzfal nem szükséges. Valójában minden egyes Internet csatlakozáskor végig kell gondolni az ebből származó biztonsági kockázatok lehetőségeit. Az ilyen kockázatok csökkentésére használható különféle módszerekről az AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00 című kiadványból tájékozódhat.  .

Célok

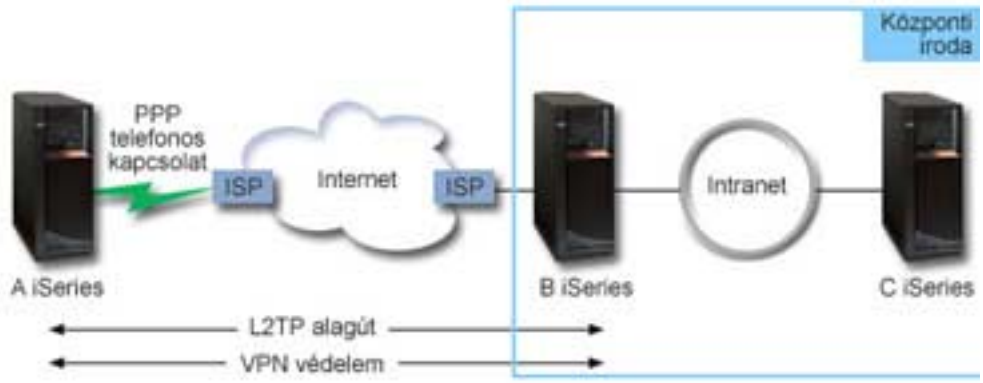
A példahelyzetben egy fiókiroda iSeries szervere VPN által védett L2TP alagúton keresztül csatlakozik a vállalati hálózat átjáró iSeries szerveréhez.

A példahelyzet fő céljai a következők:

- Mindig a fiókiroda kezdeményezi a központi iroda felé vezető kapcsolatot.
- A fiókirodában az ottani iSeries az egyetlen rendszer, amelynek hozzá kell férnie a központi iroda hálózatához. Más szavakkal a rendszer szerepe nem átjáró, hanem hoszt.
- A vállalati rendszer a központi iroda hálózatának egyik hoszt számítógépe.

Részletek

A felvázolt példahelyzet hálózatának jellemzőit az alábbi ábra szemlélteti:



A jelű iSeries

- Hozzá kell férnie a vállalati hálózat összes rendszerének TCP/IP alkalmazásaihoz.
- Az Internet szolgáltatója dinamikus IP címet biztosít számára.
- Be kell állítani L2TP támogatás nyújtására.

B jelű iSeries

- Hozzá kell férnie az A jelű iSeries szerver TCP/IP alkalmazásaihoz.
- Az alhálózat címe 10.6.0.0, a használt alhálózati maszk 255.255.0.0. Ez az alhálózat képviseli a központi irodában található VPN alagút adatvégpontját.
- Az Internetre a 205.13.237.6 címmel csatlakozik. Ez a kapcsolati végpont. Ez azt jelenti, hogy a B iSeries végzi a kulcskezelést, és alkalmazza az IPSec protokollt a kimenő és bejövő IP adatcsomagokra. A B iSeries a saját alhálózatához a 10.6.11.1 IP címmel csatlakozik.

Az L2TP szóhasználatában az *A iSeries* az L2TP kezdeményező, a *B iSeries* pedig az L2TP lezáró.

Konfigurációs feladatok

Feltételezve, hogy a TCP/IP már létezik és működik, az alábbi feladatok elvégzése szükséges:

1. Állítsa be (Lásd: 14) a VPN-t az A iSeries szerveren.
2. Állítson be egy PPP (Lásd: 16) kapcsolati profilt és egy virtuális vonalat az A iSeries szerveren.
3. Alkalmazza (Lásd: 17) a dinamikus kulcsú csoportot a PPP profilra.
4. Állítsa be (Lásd: 18) a VPN-t a B iSeries szerveren.
5. Állítson be egy PPP (Lásd: 18) kapcsolati profilt és egy virtuális vonalat a B iSeries szerveren.
6. Aktiválja (Lásd: 19) a csomagszabályokat az A és B iSeries szervereken.
7. Indítsa el (Lásd: 19) a kapcsolatot az A iSeries szerverről.

Konfiguráció részletei

A TCP/IP működésének és a szerverek kommunikációjának ellenőrzése után készen áll a példahelyzetben felvázolt kapcsolat beállításának megkezdésére.

1. lépés - A VPN beállítása az A jelű iSeries szerveren

A VPN beállításához az A iSeries szerveren tegye a következőket:

1. **Internet kulcscsere stratégia beállítása**
   a. Az iSeries navigátorban bontsa ki az A iSeries szerver **—> Hálózat —> IP stratégiák > Virtuális magánhálózatok —> IP biztonsági stratégiák** elemeket.
   b. Kattintson a jobb egérgombbal az **Internet kulcscsere stratégiák** elemre, majd válassza az előugró menü **Új Internet kulcscsere stratégia** menüpontját.

c. A **Távoli szerver** lapon válassza ki az **IPv4 cím** azonosítótípust, majd az **IP cím** mezőbe írja be a 205.13.237.6 címet.

d. A **Társítások** lapon az **Előzetesen megosztott kulcs** kiválasztásával adja meg, hogy a kapcsolat a stratégia hitelesítéséhez előzetesen megosztott kulcsot fog használni.

e. Adja meg az előzetesen megosztott kulcsot a **Kulcs** mezőben. Az előzetesen megosztott kulcsokat úgy kell kezelni, mint a jelszavakat.

f. Válassza ki a helyi kulcsszerver azonosítójának típusát a **Kulcs azonosítója** mezőben, majd adja meg a kulcsazonosítót az **Azonosító** mezőben. Például kulcsazonosító_21. Ne feledje, hogy a helyi kulcsszerver dinamikusan hozzárendelt IP címmel rendelkezik, amelyet nem lehet előre tudni. A B jelű iSeries ezzel az azonosítóval ellenőrzi az A iSeries azonosságát, amikor az a kapcsolatot kezdeményezi.

g. Az **Átalakítások** lapon kattintson a **Hozzáadás** gombra az A iSeries által a B iSeries felé felajánlott kulcsvédelmi átalakítások hozzáadásához, illetve annak meghatározásához, hogy az IKE stratégia alkalmaz-e azonosságvédelmet az 1. egyeztetési fázis kezdeményezésekor.

h. Az **IKE stratégia átalakítás** lapon válassza ki az **Előzetesen megosztott kulcs** hitelesítési módszert, az **SHA** kivonatkészítési algoritmust, és a **3DES-CBC** titkosítási algoritmust. A **Diffie-Hellman csoport** és az **IKE kulcsok érvényességi ideje** mezőkben hagyja meg az alapértelmezett értékeket.

i. Az **OK** gomb megnyomásával térjen vissza az **Átalakítások** lapra.

j. Válassza ki az **IKE agresszív módú egyeztetés (nincs azonosságvédelem)** beállítást.

k. Kattintson az **OK** gombra a konfiguráció mentéséhez.

2. **Adat stratégia beállítása**

a. A VPN felületen kattintson a jobb egérgombbal az **Adat stratégiák** elemre, majd válassza az előugró menü **Új adat stratégia** menüpontját.

b. Az **Általános** lapon adja meg az adat stratégia nevét. Például l2tp_távoli_felhasználó.

c. Kattintson az **Ajánlások** lapra. Az ajánlások olyan protokollok gyűjteményei, amelyeket a kezdeményező és válaszadó kulcsszerverek dinamikus kapcsolat kialakításához használnak két végpont között. Egy adat stratégia több kapcsolati objektumban is felhasználható. Viszont a távoli VPN kulcsszerverek nem feltétlenül azonos adat stratégia tulajdonságokkal rendelkeznek. Ennek megfelelően egy adat stratégiához több ajánlás is hozzáadható. A távoli kulcsszerver VPN kapcsolatának kialakításakor a kezdeményező és válaszadó adat stratégiájában kell lennie legalább egy megegyező ajánlásnak.

d. Kattintson a **Hozzáadás** gombra egy adat stratégia átalakítás hozzáadásához.

e. A beágyazás módjának válassza ki a **Szállítás** beállítást.

f. Adjon meg egy kulcs érvényességi értéket.

g. Az **OK** gomb megnyomásával térjen vissza az **Átalakítások** lapra.

h. Kattintson az **OK** gombra az új adat stratégia mentéséhez.

3. **Dinamikus kulcsú csoport beállítása**

4.

a. A VPN felületen bontsa ki a **Védett kapcsolatok** bejegyzést.

b. Kattintson a jobb egérgombbal a **Csoportonként** elemre, majd válassza az előugró menü **Új dinamikus kulcsú csoport** menüpontját.

c. Az **Általános** lapon adja meg a csoport nevét. Például l2tp_központ.

d. Válassza ki a **Helyi kezdeményezésű L2TP alagutat véd** beállítást.

e. A rendszer szerepének válassza ki a **Mindkét rendszer hoszt** beállítást.

f. Kattintson a **Stratégia** lapra. Az **Adat stratégia** legördülő listából válassza ki a 2. lépésben létrehozott l2tp_távoli_felhasználó nevű adat stratégiát.

g. A **Helyi rendszer kezdeményezheti a kapcsolatot** beállítás kiválasztásával adja meg, hogy csak az A iSeries kezdeményezhet kapcsolatot a B iSeries felé.

h. Kattintson a **Kapcsolatok** lapra. Válassza ki az **Alábbi stratégia szűrő előállítása a csoporthoz** lehetőséget. A stratégia szűrő paramétereinek beállításához kattintson a **Szerkesztés** gombra.

i. A **Stratégia szűrő - Helyi címek** lapon válassza ki a **Kulcsazonosító** azonosítótípust.

j. Azonosítónak válassza ki az IKE stratégiában megadott kulcsazonosító_21 kulcsazonosítót.

k. Kattintson a **Stratégia szűrő - Távoli cím** lapra. Az **Azonosító típusa** legördülő listában válassza ki az **IPv4 cím** értéket.

l. Az **Azonosító** mezőben adja meg a 205.13.237.6 címet.

m. Kattintson a **Stratégia szűrő - Szolgáltatások** lapra. A **Helyi port** és **Távoli port** mezőkbe írja be a 1701 portszámot. A 1701 az L2TP közismert portszáma.

n. A **Protokoll** legördülő listában válassza ki az **UDP** bejegyzést.

o. Az **OK** gomb megnyomásával térjen vissza a **Kapcsolatok** lapra.

p. Kattintson a **Csatolók** lapra. Válassza ki a vonalat vagy PPP profilt, amelyre a csoport vonatkozni fog. A csoport PPP profilja még nem került létrehozásra. Miután erre sor került, módosítani kell a csoport tulajdonságait, hogy a csoport a következő lépésben létrehozott PPP profilra vonatkozzon.

q. Kattintson az **OK** gombra az l2tp_központ dinamikus kulcsú csoport létrehozásához.

A létrehozott csoporthoz hozzá kell adni egy kapcsolatot.

5. **Dinamikus kulcsú kapcsolat beállítása**

   a. A VPN felületen bontsa ki a **Csoportonként** bejegyzést. Megjelenik az A iSeries szerveren beállított valamennyi dinamikus kulcsú csoport listája.

   b. Kattintson a jobb egérgombbal az **l2tp_központ** bejegyzésre, majd válassza az előugró menü **Új dinamikus kulcsú kapcsolat** menüpontját.

   c. Az **Általános** lapon megadhatja a kapcsolat leírását.

   d. A távoli kulcsszerver azonosítótípusának válassza ki az **IPv4 cím** típust.

   e. Az **IP cím** legördülő listából válassza ki a 205.13.237.6 címet.

   f. Szüntesse meg az **Indítás kérésre** beállítás kijelölését.

   g. Kattintson a **Helyi címek** lapra. Jelölje ki a **Kulcsazonosító** azonosítótípust, majd válassza ki az **Azonosító** legördülő lista kulcsazonosító_21 elemét.

   h. Kattintson a **Távoli címek** lapra. Válassza ki az **IPv4 cím** azonosítótípust.

   i. Az **Azonosító** mezőben adja meg a 205.13.237.6 címet.

   j. Kattintson a **Szolgáltatások** lapra. A **Helyi port** és **Távoli port** mezőkbe írja be a 1701 portszámot. A 1701 az L2TP közismert portszáma.

   k. A **Protokoll** legördülő listában válassza ki az **UDP** bejegyzést.

   l. Kattintson az **OK** gombra a dinamikus kulcsú kapcsolat létrehozásához.

Az A jelű iSeries szerveren befejeződött a VPN beállítása. A következő lépés egy PPP profil beállítása az A iSeries szerveren.

2. lépés - PPP kapcsolat és virtuális vonal beállítása az A iSeries szerveren

Ez a szakasz írja le a PPP profil létrehozásához az A iSeries szerveren elvégzendő lépéseket. A PPP profilhoz nincs társított fizikai vonal, hanem ehelyett virtuális vonalat használ. Ez azért van így, mert a PPP forgalom az L2TP alagúton halad át, és az L2TP alagutat VPN védi.

A PPP profil beállításához az A iSeries szerveren tegye a következőket:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries szerver —> Hálózat —> Távoli elérés szolgáltatás** elemeket.
2. Kattintson a jobb egérgombbal a **Kezdeményező kapcsolati profilok** elemre, majd válassza az előugró menü **Új profil** menüpontját.
3. A **Beállítás** lapon válassza ki a **PPP** protokolltípust.

4. A Mód kiválasztásakor adja meg az **L2TP (virtuális vonal)** beállítást.
5. A **Működési mód** legördülő listából válassza ki a **Kérésre kezdeményező (önkéntes alagút)** bejegyzést.
6. Az **OK** gomb megnyomásával haladjon tovább a PPP profil tulajdonságai párbeszédablakra.
7. Az **Általános** lapon adja meg egy olyan nevet, amely azonosítja a kapcsolat típusát és célját. Ebben az esetben adja meg például a Központhoz nevet. A megadott név legfeljebb 10 karakterből állhat.
8. Adja meg a profil leírását. (nem kötelező)
9. Kattintson a **Kapcsolat** lapra.
10. A **Virtuális vonal neve** mezőben válassza ki a legördülő lista **Központhoz** bejegyzését. Ne feledje, hogy a vonalhoz nem tartozik fizikai csatoló. A PPP profil különféle jellemzőit, például a maximális keretméretet, a hitelesítési információkat vagy a keretméretet a virtuális vonal írja le. Megjelenik az **L2TP vonal tulajdonságai** párbeszédablak.
11. Az **Általános** lapon adja meg a virtuális vonal leírását.
12. Kattintson a **Hitelesítés** lapra.
13. A **Helyi hosztnév** mezőben adja meg a helyi kulcsszerver nevét: iSeriesA.
14. Az **OK** megnyomásával mentse az új virtuális vonal leírását, és térjen vissza a **Kapcsolat** lapra.
15. A **Távoli alagút végpont címe** adja meg az alagút távoli végpontjának címét, amely a 205.13.237.6.
16. Jelölje meg az **IPSec védelmet igényel** beállítást, majd a **Kapcsolati csoport neve** legördülő listában válassza ki az 1. lépésben létrehozott l2tp_központ dinamikus kulcsú csoportot.
17. Kattintson a **TCP/IP beállítások** lapra.
18. A **Helyi IP cím** részben válassza ki a **Távoli rendszer rendeli hozzá** beállítást.
19. A **Távoli IP cím** részben válassza ki a **Rögzített IP cím használata** beállítást. Írja be a 10.6.11.1 címet, vagyis a távoli rendszer IP címét a saját alhálózatában.
20. Az Útválasztás részben válassza ki a **További statikus útvonalak meghatározása** beállítást, majd kattintson az **Útvonalak** gombra. Ha a PPP profilban nincsenek megadott útválasztási információk, akkor az A iSeries csak az alagút távoli végpontját éri el, a 10.6.0.0 alhálózat többi rendszerét nem.
21. Kattintson a **Hozzáadás** gombra egy statikus útvonal bejegyzés hozzáadásához.
22. Adja meg a 10.6.0.0 alhálózati címet és a 255.255.0.0 alhálózati maszkot a teljes 10.6.*.* forgalomnak az L2TP alagúton keresztüli továbbításához.
23. Kattintson az **OK** gombra a statikus útvonal hozzáadásához.
24. Kattintson az **OK** gombra az Útválasztás párbeszédablak bezárásához.
25. Kattintson a **Hitelesítés** lapra a PPP profil felhasználói nevének és jelszavának megadásához.
26. A Helyi rendszer azonosítása részben válassza ki a **Távoli rendszer ellenőrizheti a helyi rendszer azonosságát** beállítást.
27. A **Használandó hitelesítési protokoll** mezőben válassza ki a **Titkosított jelszó igénylése (CHAP-MD5)** beállítást.
28. Adja meg a felhasználói nevet (iSeriesA) és egy jelszót.
29. Kattintson az **OK** gombra a PPP profil mentéséhez.

3. lépés - Az l2tp_központ dinamikus kulcsú csoport alkalmazása a Központhoz PPP profilra

A PPP kapcsolati profil beállítása után vissza kell menni a létrehozott l2tp_központ dinamikus kulcsú csoporthoz, és társítani kell azt a PPP profilhoz. Ehhez tegye a következőket:

1. Keresse meg a VPN kezelőfelületet, majd bontsa ki a **Védett kapcsolatok —> Csoportonként** bejegyzést.
2. Kattintson a jobb egérgombbal az l2tp_központ dinamikus kulcsú csoportra, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kattintson a **Csatolók** lapra, majd válassza ki az **Alkalmazás a következő csoportra** beállítást és a 2. lépésben létrehozott Központhoz nevű PPP profilt.

4. Kattintson az **OK** gombra az l2tpt_központ alkalmazásához a Központhoz profilra.

4. lépés - VPN beállítása a B jelű iSeries szerveren

Kövesse az A jelű iSeries beállításának lépéseit az IP címek és azonosítók értelemszerű cseréjével. A folyamat megkezdése előtt gondolja át a következőket:

- A távoli kulcsszerver azonosítása az A iSeries szerveren a helyi kulcsszerver azonosításához megadott kulcsazonosító lesz. Például kulcsazonosító_21.
- Használja *pontosan* ugyanazt az előzetesen megosztott kulcsot.
- Győződjön meg róla, hogy az átalakítások megegyeznek az A iSeries szerveren beállítottakkal, ellenkező esetben a kapcsolat meghiúsul.
- A dinamikus kulcsú csoport **Általános** lapján ne válassza ki a **Helyi kezdeményezésű L2TP alagutat véd** beállítást.
- A kapcsolatot a távoli rendszer kezdeményezi.
- Adja meg, hogy a kapcsolat kérésre indul.

2. lépés - PPP kapcsolat és virtuális vonal beállítása a B iSeries szerveren

A PPP profil beállításához a B iSeries szerveren tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **B jelű iSeries szerver —> Hálózat —> Távoli elérés szolgáltatás** elemeket.
2. Kattintson a jobb egérgombbal a **Válaszadó kapcsolati profilok** elemre, majd válassza az előugró menü **Új profil** menüpontját.
3. A **Beállítás** lapon válassza ki a **PPP** protokolltípust.
4. A Mód kiválasztásakor adja meg az **L2TP (virtuális vonal)** beállítást.
5. A **Működési mód** legördülő listából válassza ki a **Befejező (hálózati szerver)** bejegyzést.
6. Az **OK** gomb megnyomásával haladjon tovább a PPP profil tulajdonságai párbeszédablakra.
7. Az **Általános** lapon adja meg egy olyan nevet, amely azonosítja a kapcsolat típusát és célját. Ebben az esetben adja meg például az Irodához nevet. A megadott név legfeljebb 10 karakterből állhat.
8. Adja meg a profil leírását. (nem kötelező)
9. Kattintson a **Kapcsolat** lapra.
10. Válassza ki az alagút helyi végpontjának IP címét: 205.13.237.6.
11. A **Virtuális vonal neve** mezőben válassza ki a legördülő lista **Irodához** bejegyzését. Ne feledje, hogy a vonalhoz nem tartozik fizikai csatoló. A PPP profil különféle jellemzőit, például a maximális keretméretet, a hitelesítési információkat vagy a keretméretet a virtuális vonal írja le. Megjelenik az **L2TP vonal tulajdonságai** párbeszédablak.
12. Az **Általános** lapon adja meg a virtuális vonal leírását.
13. Kattintson a **Hitelesítés** lapra.
14. A **Helyi hosztnév** mezőben adja meg a helyi kulcsszerver nevét: iSeriesB.
15. Az **OK** megnyomásával mentse az új virtuális vonal leírását, és térjen vissza a **Kapcsolat** lapra.
16. Kattintson a **TCP/IP beállítások** lapra.
17. A **Helyi IP cím** részben válassza ki a helyi rendszer rögzített IP címét: 10.6.11.1.
18. A **Távoli IP cím** részben válassza ki a **Cím tároló** cím hozzárendelési módszert. Adjon meg egy kezdőcímet, majd adja meg a távoli rendszerhez rendelhető címek számát.
19. Válassza ki a **Távoli rendszer hozzáférhet más hálózatokhoz (IP továbbítás)** beállítást.
20. Kattintson a **Hitelesítés** lapra a PPP profil felhasználói nevének és jelszavának megadásához.
21. A Helyi rendszer azonosítása részben válassza ki a **Távoli rendszer ellenőrizheti a helyi rendszer azonosságát** beállítást. Megjelenik a **Helyi rendszer azonosítása** párbeszédablak.

22. A **Használandó hitelesítési protokoll** mezőben válassza ki a **Titkosított jelszó igénylése (CHAP-MD5)** beállítást.
23. Adja meg a felhasználói nevet (iSeriesB) és egy jelszót.
24. Kattintson az **OK** gombra a PPP profil mentéséhez.

6. lépés - Csomagszabályok aktiválása

A VPN automatikusan létrehozza a kapcsolat megfelelő működéséhez szükséges csomagszabályokat. Ettől függetlenül ezeket aktiválni kell mindkét rendszeren, mielőtt a VPN kapcsolatot el lehetne indítani. Ehhez az A iSeries szerveren tegye a következőket:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries szerver —> Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomagszabályok** elemre, majd válassza az előugró menü **Aktiválás** menüpontját. Megjelenik a Csomagszabályok aktiválása párbeszédablak.
3. Válassza ki, hogy csak a VPN által előállított szabályokat vagy csak a megadott fájlban található szabályokat kívánja-e aktiválni. Megadhatja mindkét típusú szabálykészlet aktiválását is. Az utóbbi választása akkor lehet szükséges, ha rendelkezik különféle PERMIT és DENY szabályokkal, amelyeket a VPN által előállított szabályok mellett szintén érvénybe kíván léptetni a csatolón.
4. Válassza ki a csatolót, amelyen a szabályokat aktiválni kívánja. Ebben az esetben válassza a **Minden csatoló** beállítást.
5. Kattintson a párbeszédablak **OK** gombjára a szabályok ellenőrzéséhez és aktiválásához a kijelölt csatolón vagy csatolókon. Az OK gomb megnyomása után a rendszer ellenőrzi a szabályok szintaxisát, ennek eredményeit pedig a szövegszerkesztő alján található üzenet területre írja. Az adott fájlhoz és sorhoz köthető hibaüzenetek esetén kattintson a jobb egérgombbal a hibára, majd válassza az előugró menü **Ugrás sorra** menüpontját a sor kijelöléséhez.
6. A fenti lépések megismétlésével aktiválja a csomagszabályokat a B iSeries szerveren is.

7. lépés - Kapcsolat indítása

A végső lépés a kapcsolat elindítása. Az L2TP kapcsolat kezdeményezése előtt az L2TP lezárónak engedélyezni kell a válaszolást a kezdeményezési kérésekre. Az összes szükséges szolgáltatás elindulásának ellenőrzése után indítsa el a PPP kapcsolatot a lezáró oldalon. A PPP kapcsolat indításához a B iSeries szerveren tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **B jelű iSeries szerver —> Hálózat —> Távoli elérés szolgáltatás** elemeket.
2. Kattintson a **Válaszadó kapcsolati profilok** elemre a válaszadó profilok megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal az Irodához bejegyzésre, majd válassza az előugró menü **Indítás** menüpontját. A kapcsolati profil elindulása után a rendszer frissíti az ablak tartalmát, és a profil mellett a Kapcsolati kérésre várakozás állapot jelenik meg. Az A iSeries most már válaszolhat a B iSeries L2TP kapcsolati kéréseire.

Az L2TP kapcsolat indításához tegye a következőket az A jelű iSeries szerveren:

1. Az iSeries navigátorban bontsa ki az **A jelű iSeries szerver —> Hálózat —> Távoli elérés szolgáltatás** elemeket.
2. Kattintson a **Kezdeményező kapcsolati profilok** elemre a válaszadó profilok megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a **Központhoz** bejegyzésre, majd válassza az előugró menü **Indítás** menüpontját. A kapcsolati profil elindulása után a rendszer frissíti az ablak tartalmát, és a profil mellett az L2TP alagút kialakítása állapot jelenik meg.
4. Az F5 megnyomásával frissítse a képernyőt. Az L2TP alagút sikeres elindulását a kapcsolat Aktív kapcsolatok állapota jelzi.

VPN példahelyzet - Hálózati cím fordítás használata VPN kapcsolatban

A példahelyzet egy kis szegedi gyártócég helyzetét vázolja fel. Egyik üzleti partnerük, egy budapesti alkatrész beszállító a céggel végzett üzletmenet jelentős részét az Interneten kívánja a továbbiakban folytatni. Vállalatunknak rendkívül fontos, hogy a megfelelő alkatrészek a kívánt mennyiségben rendelkezésre álljanak a megfelelő időpontban, ezért a beszállítónak figyelnie kell a gyártó raktárkészletének állapotát, és a tervezett gyártási ütemezéseket. Jelenleg az interakció kezelése kézi feldolgozással történik, de ez időigényes, költséges és bizonyos esetekben pontatlan, ezért a gyártócég adminisztrátora meg szeretné vizsgálni ennek kiváltási lehetőségeit.

A cserélt információk bizalmassága és időérzékenysége miatt az adminisztrátor VPN kialakítása mellett dönt a beszállító hálózata és a gyártócég hálózata között. A belső hálózat felépítésének eltitkolása érdekében az adminisztrátor el szeretné rejteni a beszállító által használt alkalmazást futtató iSeries szerver belső IP címét. A kérdés: Hogyan oldható meg mindez?

A válasz egyszerű: az OS/400 VPN segítségével. Segítségével nemcsak a vállalati hálózaton található VPN átjáró kapcsolatmeghatározásai hozhatók létre, hanem lehetőséget nyújt a belső címek elrejtését biztosító hálózati cím fordítás beállításához is. A VPN működéséhez szükséges biztonsági megegyezések (SA) IP címeit módosító hagyományos hálózati cím fordítással (NAT) ellentétben a VPN NAT a cím fordítást még az SA ellenőrzés előtt végzi el úgy, hogy a kapcsolathoz még a kapcsolat indítása előtt kioszt egy címet.

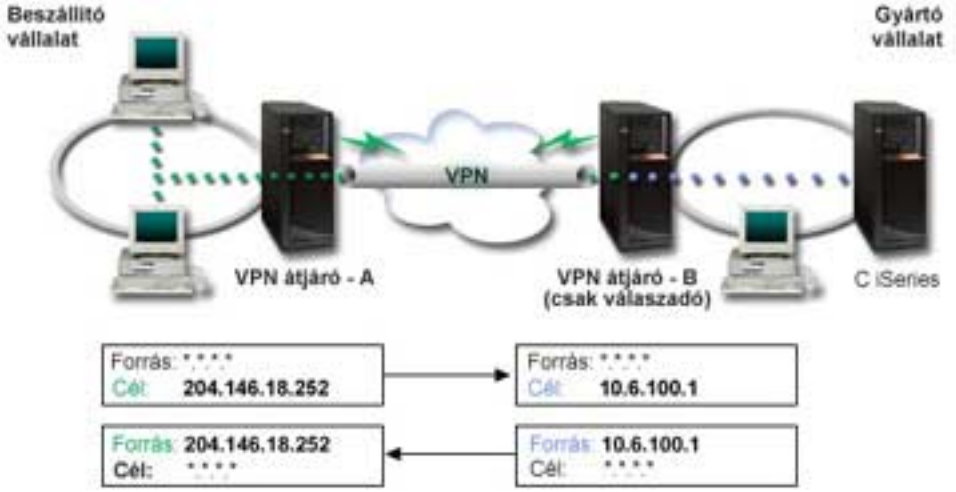
Célok

A példahelyzet céljai a következők:

- Hozzáférés biztosítása a beszállítói hálózat valamennyi kliense számára a gyártócég hálózatának egyik iSeries szerveréhez egy átjáró-átjáró VPN kapcsolaton.
- A gyártócég hálózatában lévő iSeries szerver belső IP címének elrejtése egy nyilvános IP címre való lefordításával, amelyet a VPN hálózati cím fordítás funkciója (VPN NAT) végez.

Részletek

A gyártó és a beszállító hálózatának jellemzőit az alábbi ábra szemlélteti:



- Mindig az A jelű VPN átjáró kezdeményezi a kapcsolatot a B VPN átjáróval.
- Az A VPN átjáró a kapcsolat cél végpontjának a 204.146.18.252 címet tekinti, amely a C iSeries szerverhez hozzárendelt nyilvános cím.
- A C jelű iSeries szerver belső IP címe a gyártó hálózatában 10.6.100.1.
- A B jelű VPN átjárón a helyi szolgáltatás tárolóban beállításra kerül a 204.146.18.252 cím; erre a címre lesz lefordítva a C iSeries 10.6.100.1 belső címe.

- A B jelű VPN átjáró a bejövő csomagoknál a C iSeries nyilvános címét lefordítja a 10.6.100.1 belső címre. A kimenő adatcsomagokban a C iSeries 10.6.100.1 belső IP címe a 204.146.18.252 nyilvános címre kerül lefordításra. A beszállító hálózatának szempontjából a C iSeries IP címe 204.146.18.252. Valójában nem is feltétlenül tudnak arról, hogy cím fordítás történik.

Konfigurációs feladatok

A példahelyzetben felvázolt kapcsolat beállításához a következő feladatokat kell elvégezni:

1. Alapszintű átjáró-átjáró VPN beállítása az **A** és **B** VPN átjárók között.
2. Helyi szolgáltatás tároló meghatározása a **B VPN átjárón** a **C iSeries** belső címének elrejtéséhez a 204.146.18.252 nyilvános cím mögött.
3. A **B VPN átjáró** beállítása a helyi címek lefordítására a helyi szolgáltatás tároló címeire.

VPN alapelvek

A virtuális magánhálózatok több fontos TCP/IP protokollt is felhasználnak az adatforgalom védelméhez. A VPN kapcsolatok működésének jobb megértéséhez ismernie kell ezeket a protokollokat és alapelveket, valamint azt, hogy az OS/400 VPN hogyan használja ezeket:

- **IP biztonsági (IPSec) protokollok**
  Az IPSec stabil és hosszan tartó alapot nyújt a hálózati réteg biztonságához.
- **Kulcskezelés**
  A dinamikus VPN az Internet kulcscsere (IKE) protokoll felhasználásával még biztonságosabbá teszi a kommunikációt. Az IKE lehetővé teszi a kapcsolati végpont VPN szerverek számára, hogy a megadott időközökben új kulcsokat egyeztessenek.
- **2. szintű alagútkezelési protokoll (L2TP)**
  Ha a hálózat és távoli kliensek közötti kommunikáció biztosítására kívánja használni a virtuális magánhálózatokat, akkor ismernie kell az L2TP protokollt is.
- **VPN hálózati cím fordítás (VPN NAT)**
  Az OS/400 VPN lehetőséget ad hálózati cím fordítás végzésére. A VPN által biztosított NAT abban különbözik a hagyományos hálózati cím fordítástól, hogy a címek fordítására még az IKE és IPSec protokollok alkalmazása előtt kerül sor. Ebből a témakörből szerezhet további ismereteket.
- **UDP beágyazás**
  Az UDP beágyazás lehetővé teszi az IPSec forgalomnak, hogy hagyományos NAT eszközökön haladjon át. Ebből a témakörben talál a funkcióról további információkat, és tudhatja meg, miért érdemes ezt használni a VPN kapcsolatokban.
- **IP tömörítés (IPComp)**
  Az IPComp az adatcsomagok tömörítésével csökkenti ezek méretét, így jobb kommunikációs teljesítményt biztosít a VPN partnerek között.
- **VPN és IP szűrés**
  Az IP szűrés és a VPN közeli viszonyban vannak egymással. Valójában a legtöbb VPN kapcsolat megfelelő működéséhez szükség van szűrőszabályokra. Ez a témakör mutatja be a VPN által megkövetelt szabályokat, illetve a szűrési és a VPN alapelvek egymáshoz való viszonyát.

IP biztonsági (IPSec) protokollok

Az IPSec stabil és hosszan tartó alapot nyújt a hálózati réteg biztonságához. Támogatja napjaink valamennyi kriptográfiai algoritmusát, és lehetőséget nyújt új algoritmusok használatára is, amint ezek elérhetővé válnak. Az IPSec protokollok a következő lényeges biztonsági kérdésekre nyújtanak megoldást:

Eredet hitelesítés
Ellenőrzi, hogy az adatcsomagok valóban attól származnak-e, aki ezt állítja magáról.

Integritás
Biztosítja, hogy az adatcsomagok tartalma ne változhasson meg az átvitel közben véletlen hibák vagy szándékos cselekmények hatására.

Bizalmasság
Elrejti az üzenetek tartalmát, általában valamilyen titkosítás használatával.
Újraküldés elleni védelem
Biztosítja, hogy az elfogott adatcsomagok ne legyenek újraküldhetők későbbi időpontban.
Kriptográfiai kulcsok és biztonsági megegyezések automatikus kezelése
Biztosítja, hogy a kibővített hálózaton alkalmazott VPN stratégiák csak minimális, vagy semmiféle kézi beállítást nem igényelnek.

A VPN a kapcsolaton áthaladó adatok védelmére két IPSec protokollt használ, az egyik a Hitelesítési fejléc (AH), a másik a Beágyazott biztonsági kiterjesztés (ESP). Az IPSec megvalósítás másik része az Internet kulcscsere (IKE) protokoll, más szóval a kulcskezelés. Míg az IPSec az adatok titkosítását végzi, az IKE teszi lehetővé a biztonsági megegyezések (SA) automatikus egyeztetését, illetve a kriptográfiai kulcsok automatikus előállítását és frissítését.

Az alapvető IPSec protokollok a következők:

- **Hitelesítési fejléc (AH) protokoll**
- **Beágyazott biztonsági kiterjesztés (ESP) protokoll**
- **AH és ESP protokollok kombinációja**
- **Internet kulcscsere (IKE) protokollok**

Az IETF az IPSec protokollt hivatalosan az RFC 2401 - *Security Architecture for the Internet Protocol* dokumentumban definiálja. Az RFC szövege a következő Internet címen tekinthető meg:

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

Hitelesítési fejléc (AH)

A Hitelesítési fejléc (AH) protokoll lehetővé teszi az adatok hitelesítését, integritását és újraküldés elleni védelmét. Az AH nem biztosítja viszont az adatok bizalmasságát, vagyis nem titkosítja az adatokat.

Az adatok integritásának biztosításához az AH egy üzenet hitelesítési kód, például az MD5 által előállított ellenőrző összeget használja. Az eredet hitelesítésének biztosításához az AH a hitelesítéshez használt algoritmusban felhasznál egy megosztott titkos kulcsot is. Az újraküldés elleni védelmet az AH fejléc sorozatszáma valósítja meg. Érdemes megjegyezni, hogy az említett három funkciót gyakran összevonják, és egyszerűen **hitelesítésnek** nevezik. A legegyszerűbb módon megfogalmazva az AH biztosítja, hogy az adatokba ne piszkálhassanak bele útközben.

Bár az AH az IP adatcsomagok lehető legnagyobb részét hitelesíti, az IP fejléc bizonyos mezőnek értékeit a fogadó nem jósolhatja meg. Az AH az ilyen, **változékonynak** is nevezett mezőket nem védi. Az IP csomag hasznos tartalmára ettől függetlenül mindig vonatkozik a védelem.

Az IETF a Hitelesítési fejléc (AH) protokollt hivatalosan az RFC 2402 - *IP Authentication Header* dokumentumban definiálja. Az RFC szövege a következő Internet címen tekinthető meg:

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

Lehetőségek az AH használatára

Az AH kétféleképpen alkalmazható: szállítás vagy alagút módban. Szállítás módban az adatcsomag IP fejléce a legkülső IP fejléc, ezt követi az AH fejléc, majd az adatcsomag hasznos tartalma. Az AH a változékony mezők kivételével a teljes adatcsomagot hitelesíti. A szállított adatcsomag tartalma viszont titkosítás nélkül kerül átvitelre, amely így lehallgatható. Bár a szállítás mód kisebb feldolgozási terhelést jelent az alagút módnál, az általa biztosított biztonság is alacsonyabb szintű.

Alagút módban új IP fejléc jön létre, ez lesz az adatcsomag legkülső IP fejléce. Az új IP fejlécet az AH fejléc követi. Utolsóként szerepel az eredeti adatcsomag, az IP fejlécével és az eredeti tartalmával együtt. Az AH

ebben az esetben a teljes adatcsomagot hitelesíti, ami annyit jelent, hogy a fogadó rendszer felismerheti, hogy az adatcsomag megváltozott-e a továbbítás során.

Ha a biztonsági megegyezés bármelyik végpontja átjáró, akkor alagút módot kell használni. Alagút módban a külső IP fejléc forrás- és célcímeinek nem kell megegyezniük az eredeti IP fejléc címeivel. Például két biztonsági átjáró létrehozhat egy AH alagutat az összekapcsolt hálózatok teljes forgalmának hitelesítése céljából. Valójában ez egy igen elterjedt konfiguráció.

Az alagút mód használatának előnye, hogy az alagút mód teljes mértékben védi a beágyazott IP adatcsomagot. Emellett az alagút mód lehetővé teszi saját címek használatát is.

Az AH használatának előnyei
Az adatok sok esetben igényelnek csak hitelesítést. Bár a Beágyazott biztonsági kiterjesztés (ESP) protokoll is biztosít hitelesítést, az AH nincs olyan nagy hatással a rendszer teljesítményére, mint az ESP. Az AH használatának másik előnye, hogy az AH a teljes adatcsomagot hitelesíti. Az ESP viszont nem hitelesíti a bevezető IP fejlécet, illetve az ESP fejléc előtti más információkat.

Az ESP megvalósítása ezen kívül erős kriptográfiai algoritmusokat igényel. Az erős kriptográfia bizonyos országokban korlátozott, míg az AH vonatkozásában nincsenek megkötések, tehát a világon bárhol használható.

Az AH által alkalmazott információvédelmi algoritmusok
Az AH **kivonatolt üzenet hitelesítési kód (HMAC)** algoritmusokat használ. Pontosítva a VPN a HMAC-MD5 és a HMAC-SHA algoritmusokat használja. Az MD5 és SHA algoritmusok a változó hosszúságú bemeneti adatokból és egy titkos kulcsból a bemenetre jellemző rögzített hosszúságú kimenetet hoznak létre, melynek neve kivonat érték. Ha két üzenetnek megegyezik a kivonata, akkor nagyon valószínű, hogy az üzenetek is megegyeznek. Az MD5 és az SHA is belekódolja a kimenetbe az üzenet hosszát, de az SHA biztonságosabbnak tekinthető, mivel ez hosszabb kivonatokat készít.

Az IETF a HMAC-MD5 protokollt hivatalosan az RFC 2085 - *HMAC-MD5 IP Authentication with Replay Prevention* dokumentumban definiálja. Az IETF a HMAC-SHA protokollt hivatalosan az RFC 2404 - *The Use of HMAC-SHA-1-96 within ESP and AH* dokumentumban definiálja. Az RFC dokumentumok szövege a következő Internet címen tekinthető meg: http://www.rfc-editor.org. 

Beágyazott biztonsági kiterjesztés (ESP)
A Beágyazott biztonsági kiterjesztés (ESP) protokoll bizalmasságot nyújt, emellett biztosíthat eredet hitelesítést, integritás ellenőrzést és újraküldés elleni védelmet. Az ESP és a Hitelesítési fejléc (AH) protokoll is biztosít hitelesítést, integritás ellenőrzést és újraküldés elleni védelmet, fontos különbség közöttük, hogy az ESP titkosítást is lehetővé tesz. Az ESP használatakor mindkét kommunikáló rendszer egy megosztott kulcsot használ a cserélt adatok titkosításához és visszafejtéséhez.

Ha titkosítást és hitelesítést is alkalmaz, akkor a fogadó rendszer először hitelesíti a csomagot, majd csak ennek sikere esetén folytatja a visszafejtéssel. Az ilyen konfiguráció csökkenti a fejdolgozással kapcsolatos terhelést, emellett mérsékli a szolgáltatás leállítása (DoS) támadásokkal szembeni érzékenységet.

Az ESP használatának kétféle módja
Az ESP kétféleképpen alkalmazható: szállítás vagy alagút módban. Szállítás módban az ESP fejléc az eredeti IP adatcsomag IP fejlécét követi. Ha az adatcsomag már rendelkezik egy IPSec fejléccel, akkor az ESP fejléc ez elé kerül. Az ESP befejező rész és az elhagyható hitelesítési adatok a hasznos tartalom mögé kerülnek.

A szállítási mód nem hitelesíti és titkosítja az IP fejlécet, amelyből így a támadók információkat szerezhetnek a címzéssel kapcsolatban. Bár a szállítás mód kisebb feldolgozási terhelést jelent az alagút módnál, az általa biztosított biztonság is alacsonyabb szintű. A legtöbb esetben a hosztok szállítás módban használják az ESP protokollt.

Alagút módban új IP fejléc jön létre, ez lesz az adatcsomag legkülső IP fejléce, ezt követi az ESP fejléc, majd az eredeti adatcsomag (vagyis az eredeti IP fejléc és az eredeti hasznos tartalom). Az ESP befejező rész és az elhagyható hitelesítési adatok a hasznos tartalom mögé kerülnek. Titkosítás és hitelesítés együttes alkalmazásakor az ESP teljes mértékben megvédi az eredeti adatcsomagot, mivel ilyenkor a teljes eredeti adatcsomag képezi az új ESP csomag hasznos tartalmát. Az ESP viszont nem védi az új IP fejlécet. Az átjáróknak az ESP-t alagút módban kell használniuk.

Az ESP által alkalmazott információvédelmi algoritmusok
Az ESP szimmetrikus kulcsot használ titkosításhoz, ezt használja mindkét kommunikáló fél az adatok titkosításához és visszafejtéséhez is. A küldőnek és a fogadónak a biztonságos kommunikáció megvalósítása előtt meg kell egyeznie a kulcsban. Az OS/400 VPN a titkosításhoz DES, 3DES, RC5, RC4 vagy AES algoritmust használ.

Az IETF a DES titkosítást az RFC 1829 - *The ESP DES-CBC Transform* dokumentumban definiálja hivatalosan. Az IETF a 3DES titkosítást az RFC 1851 - *The ESP Triple DES Transform* dokumentumban definiálja hivatalosan. Az RFC dokumentumok szövege a következő Internet címen tekinthető meg: http://www.rfc-editor.org. 

Az ESP a hitelesítési funkciókhoz a HMAC-MD5 vagy a HMAC-SHA algoritmusokat használja fel. Az MD5 és SHA algoritmusok a változó hosszúságú bemeneti adatokból és egy titkos kulcsból a bemenetre jellemző rögzített hosszúságú kimenetet hoznak létre, melynek neve kivonat érték. Ha két üzenetnek megegyezik a kivonata, akkor nagyon valószínű, hogy az üzenetek is megegyeznek. Az MD5 és az SHA is belekódolja a kimenetbe az üzenet hosszát, de az SHA biztonságosabbnak tekinthető, mivel ez hosszabb kivonatokat készít.

Az IETF a HMAC-MD5 protokollt hivatalosan az RFC 2085 - *HMAC-MD5 IP Authentication with Replay Prevention* dokumentumban definiálja. Az IETF a HMAC-SHA protokollt hivatalosan az RFC 2404 - *The Use of HMAC-SHA-1-96 within ESP and AH* dokumentumban definiálja. Az RFC dokumentumok szövege a következő Internet címen tekinthető meg: http://www.rfc-editor.org. 

Kombinált AH és ESP
A VPN hoszt-hoszt kapcsolatokban lehetővé teszi az AH és ESP kombinálását szállítási módban. A protokollok kombinálása a teljes IP adatcsomagot védi. Bár a két protokoll kombinációja nagyobb biztonságot nyújt, az ezzel kapcsolatos többletfeldolgozás csökkentheti az értékét.

Kulcskezelés
A VPN szerverek minden egyes sikeres hitelesítésnél ismételten előállítják a kapcsolatot védő kulcsokat, így megnehezítve a támadó dolgát, aki információkat próbál szerezni a kapcsolatból. Ha emellett a tökéletes továbbítási biztonságot is használja, akkor a támadók nem tudják kikövetkeztetni a jövőbeni kulcsokat a korábbi kulcscsomó információkból.

A VPN kulcskezelő az Internet kulcscsere (IKE) protokoll IBM megvalósítása. A kulcskezelő biztosítja a biztonsági megegyezések (SA) automatikus egyeztetését, valamint a kriptográfiai kulcsok automatikus előállítását és frissítését.

A **biztonsági megegyezések** (SA) tárolják az IPSec protokollok használatához szükséges információkat. A biztonsági megegyezések adják meg például az algoritmustípusokat, a kulcsok hosszát és élettartamát, a részvevő feleket és a beágyazási módokat.

A kriptográfiai kulcsok, amint nevük is sugallja, zárják el vagy védik meg az információkat, amíg azok el nem jutnak a rendeltetési helyükre.

Megjegyzés: A biztonságos kapcsolatok kialakításának legfontosabb tényezője a kulcsok biztonságos előállítása. Ha a kulcsok ismertté válnak, akkor minden hitelesítési és titkosítási erőfeszítés hiába.

A kulcskezelés fázisai

A VPN kulcskezelő működése két különálló fázisra osztható.

1. fázis

Az 1. fázis alakít ki egy elsődleges titkot; ebből kerülnek származtatásra az adatforgalom védelmét nyújtó későbbi kriptográfiai kulcsok. Ez akkor is igaz, ha a két végpont között még nincs biztonsági védelem. A VPN RSA aláírást vagy előzetesen megosztott kulcsot használ az egyeztetés 1. fázisának védelmére, illetve az ezt követő 2. egyeztetési fázisban cserélt IKE üzenetek védelmére szolgáló kulcsok kialakítására.

Az *előzetesen megosztott kulcsok* legfeljebb 128 karakteres nem triviális karaktersorozatok. Az előzetesen megosztott kulcsban a kapcsolat mindkét végpontjának meg kell egyeznie. Az előzetesen megosztott kulcsok előnye az egyszerűsége, hátránya viszont, hogy ezeket még az IKE egyeztetések előtt át kell adni valamilyen csatornán kívüli módszerrel, például telefonon vagy ajánlott levélben. Az előzetesen megosztott kulcsokat úgy kell kezelni, mint a jelszavakat.

Az *RSA aláíráson* alapuló hitelesítés nagyobb biztonságot nyújt az előzetesen megosztott kulcsoknál, mivel ilyenkor a hitelesítést digitális igazolások biztosítják. Használatához be kell állítani a digitális igazolásokat a Digitális igazolás kezelő (OS/400 34. opció) segítségével. Emellett bizonyos VPN megoldások RSA aláírások használatát igénylik az együttműködéshez. A 2000 VPN például RSA aláírást használ alapértelmezett hitelesítési módszerként. Mindezek mellett az RSA aláírások jobb méretezhetőséget biztosítanak az előzetesen megosztott kulcsoknál. A felhasznált igazolásoknak olyan Igazolási hatóságtól kell származnia, amelyben mindkét kulcsszerver megbízik.

2. fázis

A 2. fázisban történik az alkalmazások adatcseréjének védelmét szolgáló biztonsági megegyezések és kulcsok egyeztetése. Ne feledje, hogy eddig a pontig még semmilyen alkalmazásfüggő adat küldésére nem került sor. Az IKE 2. fázisának üzeneteit az 1. fázis védi.

A 2. egyeztetési fázis befejezésekor a VPN biztonságos és dinamikus kapcsolattal rendelkezik a hálózaton a kapcsolatban megadott végpontok között. A VPN kapcsolaton áthaladó adatok a kulcsszerverek által az egyeztetés 1. és 2. fázisában meghatározott biztonsági intézkedések védelme alatt állnak.

Az 1. egyeztetési fázisra általában naponta egyszer kerül sor, míg a 2. fázisra óránként, de beállítható akár 5 perces egyeztetési időszak is. A magasabb frissítési gyakoriság egyfelől növeli az adatbiztonságot, másrészt viszont csökkenti a rendszer teljesítményét. A legérzékenyebb adatok védelméhez használjon rövid kulcs élettartamokat.

Amikor az iSeries navigátorban létrehoz egy dinamikus VPN-t, akkor meg kell határozni egy IKE stratégiát az 1. egyeztetési fázishoz, illetve egy adat stratégiát a másodikhoz. Használhatja az Új kapcsolat varázslót is. A varázsló automatikusan létrehozza a VPN megfelelő működéséhez szükséges valamennyi konfigurációs objektumot, beleértve az IKE stratégiát és az adat stratégiát.

Ajánlott információforrások

A további részletekre is kíváncsi az Internet kulcscsere (IKE) protokollról és a kulcskezelésről, akkor érdemes elolvasni az IETF alábbi RFC dokumentumait:

- 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)*

Az RFC dokumentumok szövege a következő Internet címen tekinthető meg: http://www.rfc-editor.org. 

2. szintű alagútkezelési protokoll (L2TP)

A virtuális vonalaknak is nevezett L2TP kapcsolatok költséghatékony hozzáférést biztosítanak a távoli felhasználók számára azáltal, hogy lehetővé teszik a vállalati hálózat szervereinek a távoli felhasználókhoz hozzárendelt IP címek kezelését. Ezen kívül az L2TP kapcsolatok IPSec védelem használata esetén biztonságos hozzáférést nyújtanak a rendszerhez vagy hálózathoz.

Az L2TP kétféle alagút módot támogat: az önkéntes és a kötelező alagutakat. A kétféle alagút mód között a leglényegesebb különbség a végpont. Az önkéntes alagút a távoli kliensnél, míg a kötelező alagút az Internet szolgáltatónál fejeződik be.

Az L2TP **kötelező alagutak** esetén a távoli hoszt kapcsolatot kezdeményez az Internet szolgáltatójához. Az Internet szolgáltató ezután kialakít egy L2TP kapcsolatot a távoli felhasználó és a vállalati hálózat között. Bár a kapcsolatot az Internet szolgáltató alakítja ki, a VPN használatával a felhasználó határozhatja meg a forgalom védelmét. Kötelező alagutak használatához az Internet szolgáltatónak támogatnia kell az L2TP protokollt.

Az L2TP **önkéntes alagutak** esetén a kapcsolatot a távoli felhasználó hozza létre, általában egy L2TP alagútkezelési klienssel. Ennek eredményeként a távoli felhasználó az L2TP csomagokat az Internet szolgáltatójának küldi, amely továbbítja azokat a vállalati hálózat felé. Önkéntes alagutak esetén az Internet szolgáltatónak nem kell támogatnia az L2TP protokollt. Az *L2TP önkéntes alagút védelme IPSec megoldással* példahelyzet bemutat egy példát, hogyan köthető össze VPN által védett L2TP alagúttal egy fiókiroda iSeries szervere a vállalati hálózattal egy átjáró iSeries szerveren keresztül.

Az L2TP valójában az IP beágyazási protokolloknak egy változata. Az L2TP alagút úgy jön létre, hogy minden L2TP keret egy Felhasználói adatcsomag protokoll (UDP) csomagba kerül, amely pedig egy IP csomagba kerül beágyazásra. A kapcsolat végpontjait ennek az IP csomagnak a forrás- és célcíme határozza meg. Mivel a külső beágyazási protokoll IP, az összetett csomagra alkalmazhatók az IPSec protokollok. Ez védi az L2TP alagútban forgalmazott adatokat. Ezután a szokásos módon alkalmazhatók a Hitelesítési fejléc (AH), Beágyazott biztonsági kiterjesztés (ESP) és Internet kulcscsere (IKE) protokollok.

Hálózati cím fordítás VPN kapcsolatokban

A hálózati cím fordítás (NAT) a belső IP címeket nyilvános IP címekre fordítja le. Ez egyrészről segít megőrizni az értékes nyilvános címeket, másrészről lehetővé teszi a privát hálózat belső IP címeket használó hosztjainak az Internet (vagy más nyilvános hálózat) hosztokon biztosított szolgáltatások igénybe vételét.

Belső IP címek használatakor továbbá ezek ütközhetnek hasonló bejövő címekkel. Ha például kommunikálni kíván egy másik hálózattal, de mindkét hálózat 10.*.*.* címeket alkalmaz, akkor a címek ütközése miatt minden csomag eldobásra kerül. A NAT alkalmazása a kimenő címekre úgy tűnik, hogy megoldja ezt a problémát. Ha azonban az adatforgalmat VPN védi, akkor a hagyományos NAT nem működik, mivel módosítja a VPN működéséhez szükséges biztonsági megegyezések (SA) IP címeit. Ezen probléma elkerüléséhez a VPN saját hálózati cím fordítási szolgáltatást nyújt, amelynek neve VPN NAT. A VPN NAT a cím fordítást még az SA ellenőrzés előtt végzi el úgy, hogy a kapcsolathoz még a kapcsolat indítása előtt kioszt egy címet. Ez a cím a kapcsolat törléséig továbbra is a kapcsolathoz tartozik.

Megjegyzés: Az FTP jelenleg nem támogatja a VPN NAT funkciót.

A VPN NAT használata

Mielőtt megkezdené használatukat, megjegyezzük, hogy a VPN hálózati cím fordításnak kétféle változata van. Ezek a következők:

VPN NAT az IP cím ütközések kiküszöböléséhez
A VPN NAT ezen típusa lehetővé teszi az esetleges IP cím ütközésekkel kapcsolatos problémák elkerülését az olyan esetekben, amikor a hálózatot hasonló címzési renddel rendelkező hálózathoz csatlakoztatja. Ennek tipikus példája az, amikor két, a saját hálózatában szabványos belső IP címeket

használó vállalat VPN kapcsolatot szeretne kialakítani a hálózataik között. Ilyen IP cím például a 10.*.*.* vagy a 192.168.*.*. Az ilyen jellegű VPN NAT beállításának módja attól függ, hogy a helyi szerver a VPN kapcsolat kezdeményezője vagy válaszadója-e. Ha a saját szerver a kapcsolat kezdeményezője, akkor a helyi címek lefordíthatók olyanokra, amelyek kompatibilisek a VPN kapcsolati partner címeivel. Ha a saját szerver a kapcsolatban válaszadó, akkor a VPN partner távoli címei lefordíthatók olyan címekre, amelyek nem ütköznek a helyi hálózaton alkalmazott címtartománnyal. Ilyen jellegű címfordítást csak dinamikus kapcsolatokban állítson be.

VPN NAT a helyi címek elrejtéséhez
A VPN NAT ezen típusát elsősorban arra használják, hogy elrejtse a helyi rendszer tényleges IP címét úgy, hogy a cím lefordításra kerül egy nyilvánosan hozzáférhető címre. A VPN NAT beállításakor megadható, hogy minden egyes nyilvánosan ismert IP cím lefordításra kerüljön egy rejtett címeket tartalmazó címkészlet valamelyik címére. Ez lehetővé teszi egy egyedi cím terhelésének kiegyenlítését több cím között. A VPN NAT a helyi címeknél megköveteli, hogy a saját szerver a kapcsolatok válaszadója legyen.

A VPN hálózati cím fordítást akkor használja a helyi címek elrejtésére, ha az alábbi kérdésekre igennel válaszol:

1. Rendelkezik olyan szerverekkel, amelyekhez a felhasználóknak VPN használatával kellene hozzáférniük?
2. Rugalmasnak kell lenni a rendszerek tényleges IP címeivel kapcsolatban?
3. Rendelkezik legalább egy globálisan továbbítható IP címmel?

A *Hálózati cím fordítás használata VPN kapcsolatban* példahelyzet mutat be egy példát arra, hogyan állítható be a VPN NAT egy iSeries szerver helyi címeinek elrejtésére.

A VPN NAT beállítására vonatkozó részletes útmutatásokat az iSeries navigátor VPN felületének online súgójából tudhatja meg.

NAT-kompatibilis IPSec

A probléma: A hagyományos NAT megszakítja a VPN kapcsolatot
A hálózati cím fordítás (NAT) lehetővé teszi a bejegyzetlen saját IP címek elrejtését egy vagy több bejegyzett IP cím mögött. Ez segít megvédeni a belső hálózatot a külső hálózatoktól. A NAT emellett segít az IP címek fogyásának kezelésében is, mivel segítségével több saját cím is ábrázolható igen kevés regisztrált címmel.

Sajnálatos módon azonban a hagyományos NAT nem működik az IPSec csomagokon, mivel a NAT eszközön áthaladáskor megváltozik a csomag forráscíme, amely érvényteleníti a VPN csomagokat. Ebben az esetben a VPN fogadó végpontja dobja a csomagot, és a VPN kapcsolati egyeztetések meghiúsulnak.

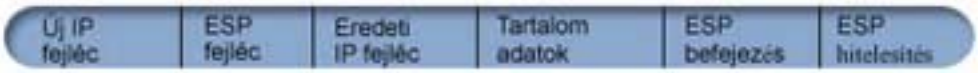
A megoldás: UDP beágyazás
Az UDB beágyazás lényege dióhéjban az, hogy az IPSec csomagot egy új UDP csomagba helyezi, amely új UDP/IP fejlécet kap. Az új IP fejlécben szereplő cím kerül lefordításra, amikor a csomag áthalad a NAT eszközön. Ezután amikor a csomag eléri a célját, a fogadó fél leválasztja a kiegészítő fejlécet, meghagyva az eredeti IPSec csomagot, amelynek meg kell felelnie minden ellenőrzéseknek.

Az UDP beágyazás csak az olyan VPN kapcsolatokban használható, amelyek az IPSec ESP protokolljának használatát adják meg alagút vagy szállítás módban. Emellett a V5R2 kiadásban az iSeries szerver az UDP beágyazásnak csak a kliense lehet. Ez annyit tesz, hogy az UDP-beágyazott forgalomnak csak a *kezdeményezésére* képes.

Az alábbi ábrák az UDP-beágyazott alagút módú ESP csomagokat szemléltetik:

Eredeti IPv4 adatcsomag:

Alagút módú ESP alkalmazása után:



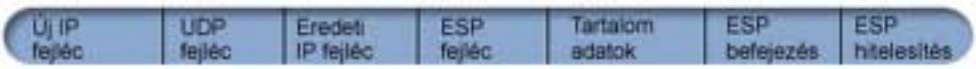
UDP beágyazás alkalmazása után:

Az alábbi ábrák az UDP-beágyazott szállítás módú ESP csomagokat szemléltetik:

Eredeti IPv4 adatcsomag:

Szállítás módú ESP alkalmazása után:

UDP beágyazás alkalmazása után:



A csomagot a beágyazás után az iSeries átküldi a VPN partnernek az 500-as UDP porton. Ne feledje, hogy a VPN partnerek az IKE egyeztetéseket is az 500-as UDP porton végzik. Az UDP-beágyazott forgalom azonos porton küldése esetén a VPN partnereknek nem kell további portokat megnyitniuk a tűzfalon és nincs szükség a kapcsolat forgalmát engedélyező új csomagszabályok írására sem. A kapcsolat fogadó végpontja könnyedén megállapíthatja, hogy a csomag IKE vagy UDP-beágyazott csomag, mivel az UDP-beágyazott csomagokban az UDP hasznos tartalom első 8 byte-ja nullára van állítva. A megfelelő működés érdekében a kapcsolat mindkét végpontjának támogatnia kell az UDP beágyazást. «

IP tömörítés (IPComp)

Az IP tömörítési protokoll (IPComp) az adatcsomagok tömörítésével csökkenti ezek méretét, így jobb kommunikációs teljesítményt biztosít a partnerek között. A protokoll szándéka a teljes kommunikációs teljesítmény javítása az olyan esetekben, amikor a kommunikáció lassú vagy torlódott összeköttetéseken folyik. Az IPComp semmiféle biztonságot nem nyújt, ezért ha a kommunikáció VPN kapcsolatban folyik, akkor egy AH vagy ESP átalakítással együtt kell felhasználni.

Az IETF az IPComp protokollt hivatalosan az RFC 2393 - *IP Payload compression Protocol (IPComp)* dokumentumban definiálja. Az RFC szövege a következő Internet címen tekinthető meg:

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

VPN és IP szűrés

» A legtöbb VPN kapcsolat megfelelő működéséhez szükség van szűrőszabályokra. A szükséges szűrőszabályok a VPN kapcsolat típusától, illetve a felügyelni kívánt forgalom jellegétől függnek. Általában minden kapcsolat rendelkezik egy stratégia szűrővel. A stratégia szűrő határozza meg, hogy a VPN-t milyen

címek, protokollok és portok használhatják. Ezen felül az Internet kulcscsere (IKE) protokollt támogató kapcsolatok általában rendelkeznek olyan szabályokkal, amelyek kifejezetten engedélyezik az IKE feldolgozást a kapcsolaton belül.

Az operációs rendszer V5R1 kiadásától kezdődően a VPN képes ezen szabályok automatikus előállítására. Amikor csak lehet, hagyja, hogy a VPN előállítsa a stratégia szűrőket. Ez nemcsak a hibák kiküszöböléséhez nyújt segítséget, hanem ilyenkor nincs szükség arra, hogy a szabályokat külön lépésben összeállítsa az iSeries navigátor csomagszabály szerkesztőjével.

Természetesen vannak kivételek is. Az alábbi témakörök leírnak néhány további, kevésbé általános koncepciót és technikát a VPN és a szűrés vonatkozásában, amelyek bizonyos helyzetekben hasznosak lehetnek:

- **Stratégia szűrők átvétele az aktuális kiadásra**
  Az operációs rendszer V4R4 és V4R5 kiadásában a VPN csomagszabályokat külön lépésben kellett beállítani. Más szóval az előállításukra nem került sor automatikusan a VPN beállításának részeként. Ez a témakör járja körül a V4R4 és V4R5 stratégia szűrőknek az aktuális kiadásra átvételével kapcsolatos speciális szempontokat, illetve írja le az áttérés folyamatát.
- **Stratégia szűrők nélküli VPN kapcsolatok**
  Ha a VPN kapcsolati végpontjai egyedülálló adott IP címek, és a virtuális magánhálózatot csomag szabályok megírása vagy aktiválása nélkül kívánja elindítani, akkor beállíthat egy dinamikus stratégia szűrőt. Ez a témakör tárgyalja az említett helyzet indikációit, és körvonalazza a megvalósítását.
- **Implicit IKE**
  Ahhoz, hogy a VPN kapcsolatok képesek legyenek IKE egyeztetésekre, engedélyezni kell az UDP forgalmat az 500-as porton. Ha azonban a rendszeren nincsenek kifejezetten az IKE forgalom engedélyezését szolgáló szűrőszabályok, akkor a rendszer engedélyezi az IKE forgalmat. Ebben a témakörben szerezhet további információkat ennek működéséről. «

Stratégia szűrők átvétele az aktuális kiadásra

Az operációs rendszer V4R4 és V4R5 kiadásában a VPN csomagszabályokat külön lépésben kellett beállítani az iSeries navigátor csomagszabály szerkesztőjében. Más szóval az előállításukra nem került sor automatikusan a VPN beállításának részeként. Az operációs rendszer V5R1 kiadásától kezdődően a VPN felület képes ezen csomagszabályok automatikus létrehozására.

Több dolgot is meg kell fontolni ha a V4R4 vagy V4R5 kiadásban létrehozott stratégia szűrőszabályokat (IPSEC tevékenységet megadó szabályokat) az aktuális kiadásban is használni kívánja. Szintén át kell gondolni az olyan helyzeteket, amikor a VPN *előállítja* a stratégia szűrőszabályokat, de ezeket ki kívánja egészíteni más IP forgalmat (például Telnet) engedélyező szabályokkal is. A lehetséges konfigurációs hibák elkerülése érdekében mindig tartsa be a következő tanácsokat.

Tisztázás képpen: A témakörben a *felhasználói* szabályfájlok olyan szabályfájlokat jelentenek, amelyek létrehozására az iSeries navigátor csomagszabály szerkesztőjének használatával került sor. Ennek ellentéte a *VPNPOLICYFILTERS.I3P* szabályfájl, amelyben a VPN által a VPN beállítások részeként automatikusan előállított szabályok találhatók.

- Ha rendelkezik V4R4 vagy V4R5 kiadásban létrehozott VPN kapcsolatokkal, és nem tervezi további VPN kapcsolatok beállítását az aktuális kiadásban, akkor a szűrőszabályok aktiválását és a kapcsolatok indítását végezheti az eddig megszokottaknak megfelelően.
- » Ha vannak V4R4 vagy V4R5 kiadásban létrehozott kapcsolatai, és további VPN kapcsolatok beállítását tervezi az aktuális kiadásban, akkor használnia kell a **Stratégia szűrők átvétele** varázslót. A varázsló eltávolítja a stratégia szűrőket a létrehozott csomagszabály fájlokból, és elhelyezi az ezeknek megfelelő stratégia szűrőket a VPN által előállított VPNPOLICYFILTERS.I3P fájlba. A varázsló elindításához tegye a következőket:
  1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
  2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Stratégia szűrők átvétele** menüpontját.

3. A varázsló befejezésekor kattintson a **Befejezés** gombra.
4. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra. «

- Ha a VPN előállított a stratégia szűrőszabályokat, de további nem VPN szűrőszabályokat kíván hozzáadni, akkor ezeket a szabályokat az iSeries navigátor Csomagszabály szerkesztőjében kell beállítania. Ha ezen nem VPN szűrőszabályoknak meg kell előzniük a VPN szűrőket, akkor a készletük nevének a PREIPSEC direktívával kell kezdődnie, például PREIPSEC_SAJÁT_SZABÁLYOK. Ez teszi lehetővé a rendszernek a szabályok feldolgozási sorrendjének meghatározását. A többi nem VPN szabály nevének kezdete nem lehet PREIPSEC. Egy alternatív név lehet például a TOVÁBBI_SZABÁLYOK.
- Mindig engedélyezni kell a VPN számára a stratégia szűrőszabályok létrehozását. A nem VPN szűrőszabályoknak viszont a felhasználói szabályfájlban kell maradniuk. Ne feledje, ha bármely nem VPN szűrőnek a VPNPOLICYFILTERS.I3P fájlban található stratégia szűrők előtt kell betöltődnie, akkor a szűrőkészlet nevéhez hozzá kell fűzni a PREIPSEC előtagot. Ez biztosítja, hogy a felhasználói szabályok és a VPN szabályai megfelelően működjenek együtt. Példaként tekintsünk egy olyan helyzetet, amelyben stratégia szűrőszabályokat (VPN készletek) a VPN állította elő, de hozzáadott további szabályokat is (saját készletek) más IP forgalom engedélyezése érdekében. A szabályok betöltésekor a sorrendjük a következő lesz:
  1. PREIPSEC kezdetű saját készletek
  2. PREIPSEC kezdetű VPN készletek
  3. ACTION=IPSEC meghatározással rendelkező VPN készletek (stratégia szűrők)
  4. ACTION=IPSEC meghatározással rendelkező saját készletek (stratégia szűrők)
  5. Tetszőleges egyéb saját készletek
  6. Tetszőleges egyéb VPN készletek

  Az összefűzött kimeneti sorrendjét az EXPANDED.OUT fájlban tekintheti meg. Az EXPANDED.OUT fájl a felhasználói szabályfájlt tartalmazó katalógusba kerül.
- » Az iSeries navigátorban a következő szabályok aktiválására van lehetőség:
  - csak a VPN által előállított VPNPOLICYFILTERS.I3P szabályfájl
  - csak a felhasználói szabályfájl
  - A VPN által előállított szabályok és a felhasználói szabályfájl is «
- A saját szűrőszabályokat egyedi csatolók helyett minden csatolón aktiválja. Ez biztosítja, hogy a szűrők aktiválásra kerülnek, és ez állítja be a stratégia szűrők megfelelő sorrendjét is.
- A szűrőszabályokat mindig ellenőrizze az aktiválásuk előtt. Ha az ellenőrzés hibák nélkül lefut, akkor az EXPANDED.OUT fájl megtekintésével győződjön meg róla, hogy a sorrendjük megfelel az elképzeléseknek. Az ellenőrzési lépés befejezése után aktiválhatja a szabályokat.

Stratégia szűrők nélküli VPN kapcsolatok

» A stratégia szűrőszabályok határozzák meg, hogy milyen címek, protokollok és portok használhatják a VPN kapcsolatot, és irányítják a megfelelő forgalmat a kapcsolaton belül. Bizonyos esetekben olyan kapcsolatok is beállíthatók, amelyek nem igényelnek stratégia szűrőszabályt. Lehetnek például betöltött nem VPN szabályok a VPN kapcsolat által használt csatolón, így a csatoló aktív szabályainak leállítása helyett dönthet a VPN olyan beállítása mellett, amelyben a rendszer dinamikusan kezeli a kapcsolat minden szűrőjét. Az ilyen típusú kapcsolatok stratégia szűrőit **dinamikus stratégia szűrőknek** hívjuk. Dinamikus stratégia szűrők használatához teljesülniük kell a következő feltételeknek:

- A kapcsolatot csak a helyi szerver kezdeményezheti.
- A kapcsolat adatvégpontjai csak egyedülálló rendszerek lehetnek. Vagyis nem lehet alhálózat vagy címtartomány.
- A kapcsolathoz nem tölthető be stratégia szűrőszabály.

Ha a kapcsolat megfelel a feltételeknek, akkor beállítható úgy, hogy ne igényeljen stratégia szűrőt. A kapcsolat indításakor megindul az adatvégpontok közötti forgalom, függetlenül a rendszeren betöltött többi csomagszabálytól.

A stratégia szűrőket nem igénylő VPN kapcsolatok beállítására vonatkozó részletes útmutatásokat az iSeries navigátor VPN felületének online súgójából tudhatja meg. «

Implicit IKE

» A kapcsolat kialakításához a legtöbb VPN kapcsolatnak szüksége van Internet kulcscsere (IKE) egyeztetésekre az IPSec feldolgozás megkezdése előtt. Az IKE a közismert 500-as portot használja, tehát az IKE megfelelő működésének biztosításához engedélyezni kell az UDP forgalmat az 500-as porton. Ha a rendszeren nincsenek kifejezetten az IKE forgalom engedélyezését szolgáló szűrőszabályok, akkor az IKE forgalom hallgatólagosan megengedett. A kifejezetten az 500-as UDP portra írt szabályok kezelése viszont az aktív szűrőszabályok előírásai alapján történik. «

VPN tervezés

A tervezés a VPN sikeres használatának kulcsfontosságú eleme. A kapcsolat megfelelő működésének biztosításához több összetett döntést is meg kell hozni. A VPN sikeres használatának biztosításához szükséges információk összegyűjtéséhez használja a következő erőforrásokat:

- **VPN beállítási követelmények**
  Mielőtt megkezdi, meg kell győződnie arról, hogy a környezet megfelel a VPN létrehozására vonatkozó minimális követelményeknek.
- **Létrehozandó VPN típusának meghatározása**
  A sikeres tervezés első fontos lépése a VPN felhasználási módjának meghatározása. Ez a témakör írja le a különféle beállítható kapcsolattípusokat.
- **VPN tervezési tanácsadó**
  A tervezési tanácsadó feltesz néhány kérdést a hálózatról, és a válaszok alapján tanácsokkal látja el a VPN létrehozásával kapcsolatban.
  Megjegyzés: A VPN tervezési tanácsadót csak olyan kapcsolatokhoz használja, amelyek támogatják az Internet kulcscsere (IKE) protokollt. A kézi kapcsolattípusokhoz használja a kézi kapcsolatok tervezési munkalapjait.
- **VPN tervezési munkalapok kitöltése**
  Igény szerint kinyomtathatja és kitöltheti a tervezési munkalapokat, amelyeken összegyűjtheti a VPN tervezéssel kapcsolatos különféle információkat.

A VPN megvalósításának megtervezése után megkezdheti a VPN beállítását.

VPN beállítási követelmények

Az iSeries szerver és a hálózati kliensek megfelelő működésének érdekében győződjön meg róla, hogy az iSeries és a PC megfelel a következő követelményeknek:

V5R2 iSeries követelmények

- OS/400 (5722-SS1) V5R2 vagy újabb
- Digitális igazolás kezelő (5722-SS1 34. opció)
- Cryptographic Access Provider (5722-AC2 vagy AC3)
- iSeries Access for Windows(5722-XE1) és iSeries navigátor
  - Az iSeries navigátor Hálózat részösszetevője
- A Szerver biztonsági adatok megtartása (QRETSVRSEC *SEC) rendszerváltozó értéke 1
- A TCP/IP be van állítva, beleértve az IP csatolókat, útvonalakat, helyi hosztnevet és a helyi tartománynevet

Kliens követelmények

- 32 bites Windows operációs rendszert futtató munkaállomás, amely TCP/IP protokollal csatlakozik az iSeries szerverre
- 233 MHz processzor
- 32 MB RAM Windows 95/98 kliensek esetén
- 64 MB RAM Windows NT és 2000 kliensek esetén
- A kliens számítógépen telepítve van az iSeries Access for Windows és az iSeries navigátor
- IPSec protokollt támogató szoftver
- L2TP protokollt támogató szoftver, amennyiben a távoli felhasználók L2TP kapcsolatokat alakítnak ki a rendszerrel

Létrehozandó VPN típusának meghatározása

A sikeres tervezés első fontos lépése a VPN felhasználási módjának meghatározása. Ehhez meg kell értenie a helyi és a távoli kulcsszerver szerepét is a kapcsolaton belül. Például hogy a *kapcsolati* végpontok különböznek-e az *adat*végpontoktól. Azonosak, vagy valamilyen kombinációban mindkettő előfordul? A kapcsolati végpontok hitelesítik és titkosítják (vagy fejtik vissza) a kapcsolat adatforgalmát, továbbá az Internet kulcscsere (IKE) protokollal a kulcsok kezelését is biztosíthatják. Az adatvégpontok határozzák meg a VPN összeköttetésen folyó IP forgalom két rendszere közötti kapcsolatot, például a 123.4.5.6 és 123.7.8.9 közötti valamennyi TCP/IP forgalom. Általában amikor a kapcsolati és adatvégpontok eltérőek, akkor a VPN szerver átjáró. Amikor megegyeznek, akkor a VPN szerver hoszt.

A legtöbb üzleti igénynek megfelelő VPN megvalósítási típusok a következők:

Átjáró-átjáró
A kapcsolati végpontok mindkét rendszeren eltérnek az adatvégpontoktól. Az IP biztonsági (IPSec) protokoll az átjárók között folyó adatforgalmat védi. Nem biztosítja viszont az adatok védelmét egyik átjáró helyi hálózatában sem. Ez a telephelyek között alkalmazott kapcsolatok általános helyzete, mivel a két telephely átjárója mögötti helyi hálózat gyakran megbízhatónak tekinthető.

Átjáró-hoszt
Az IPSec a helyi hálózati átjáró és a távoli hálózati hoszt közötti adatforgalmat védi. A VPN nem védi a helyi hálózat adatforgalmát, mivel ez megbízhatónak tekinthető.

Hoszt-átjáró
A VPN a helyi hálózat egyik hosztja és egy távoli átjáró közötti adatforgalmat védi. A VPN nem védi a távoli hálózat adatforgalmát.

Hoszt-hoszt
A kapcsolat mindkét végpontja azonosan adatvégpont a helyi és a távoli rendszeren is. A VPN a helyi hálózati és a távoli hálózati hoszt közötti adatforgalmat védi. Az ilyen VPN végpont-végpont IPSec védelmet biztosít.

VPN tervezési munkalapok kitöltése

A VPN tervezési munkalapok segítségével gyűjtheti össze a VPN használatra vonatkozó részletes információkat. Az információkra a megfelelő VPN stratégia kialakítása miatt van szükség. Emellett az információk a VPN beállításakor is felhasználhatók. Válassza ki a létrehozni kívánt kapcsolattípusnak megfelelő munkalapot.

- **Dinamikus kapcsolatok tervezési munkalapja**
  Ezt a munkalapot töltse ki dinamikus kapcsolatok beállítása előtt.
- **Kézi kapcsolatok tervezési munkalapja**
  Ezt a munkalapot töltse ki kézi kapcsolatok beállítása előtt.
- **VPN tervezési tanácsadó**
  Ha további segítségre van szüksége, akkor használhatja a tanácsadó által nyújtott interaktív tervezési és konfigurációs segédletét is. A tervezési tanácsadó feltesz néhány kérdést a hálózatról, és a válaszok alapján tanácsokkal látja el a VPN létrehozásával kapcsolatban.

Megjegyzés: A VPN tervezési tanácsadót csak dinamikus kapcsolatokhoz használja. A kézi kapcsolattípusokhoz használja a kézi kapcsolatok tervezési munkalapjait.

Ha több hasonló tulajdonságokkal rendelkező kapcsolatot fog létrehozni, akkor érdemes beállítani a VPN alapértelmezéseket. A VPN adatlapok mezőiben az alapértelmezett értékek fognak megjelenni. Ez azt jelenti, hogy az azonos tulajdonságokat elég csak egyszer beállítani. A VPN alapértelmezések beállításához válassza a VPN felület **Szerkesztés** menüjének **Alapértelmezések** menüpontját.

Dinamikus kapcsolatok tervezési munkalapja

Dinamikus VPN kapcsolatok létrehozása előtt töltse ki az alábbi munkalapot. A munkalap az Új kapcsolat varázsló használatát feltételezi. A varázsló a megadott alapvető biztonsági követelményeken alapuló VPN kapcsolatok létrehozását teszi lehetővé. Bizonyos esetekben elképzelhető, hogy a varázsló által létrehozott konfiguráció kézi pontosítást igényel. A későbbiek során például úgy dönthet, hogy naplózást kíván végezni a VPN szerveren, vagy el kívánja indítani a VPN szervert a TCP/IP indításakor. Ebben az esetben kattintson a jobb egérgombbal a varázsló által létrehozott dinamikus kulcsú csoporton vagy kapcsolaton, majd válassza az előugró menü **Tulajdonságok** menüpontját.

A VPN beállításának megkezdése előtt minden kérdést válaszoljon meg.

Előfeltétel ellenőrzőlista	**Válaszok**
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	
A Digitális igazolás kezelő (5722-SS1, 34. opció) telepítve van?	
Van telepített Cryptographic Access Provider (5722-AC2 vagy AC3) termék?	
Telepítve van az iSeries Access for Windows (5722-XE1) termék?	
Telepítve van az iSeries navigátor?	
Telepítve van az iSeries navigátor Hálózat részösszetevője?	
Telepítve van a TCP/IP Connectivity Utilities for OS/400 (5722-TC1) termék?	
Beállította a Szerver biztonsági adatok megtartása (QRETSVRSEC *SEC) rendszerváltozót 1-re?	
Be van állítva a TCP/IP az iSeries szerveren (beleértve az IP csatolókat, útvonalakat, a helyi hosztnevet és a helyi tartománynevet)?	
A szokásos TCP/IP kommunikáció működik a szükséges végpontok között?	
Alkalmazta a legújabb ideiglenes program javításokat (PTF)?	
Ha a VPN alagút forgalma tűzfalakon vagy IP csomagszűrést megvalósító útválasztókon halad át, akkor támogatja a tűzfal vagy útválasztó az AH és ESP protokollokat?	
A tűzfalak vagy útválasztók be vannak állítva az IKE (UDP 500-as port), AH és ESP protokollokhoz?	
A tűzfalakon be van állítva az IP továbbítás?	

A dinamikus VPN kapcsolat beállításához szükséges információk	**Válaszok**
Milyen típusú kapcsolatot hoz létre? • Átjáró-átjáró • Hoszt-átjáró • Átjáró-hoszt • Hoszt-hoszt	
Mi lesz a dinamikus kulcsú csoport neve?	

Milyen biztonságot és rendszerteljesítményt követel meg a kulcsok védelméhez? • Legnagyobb biztonság, legkisebb teljesítmény • Kiegyensúlyozott biztonság és teljesítmény • Legkisebb biztonság, legnagyobb teljesítmény	
Igazolásokat használ a kapcsolat hitelesítéséhez? Ha nem, akkor mi az előzetesen megosztott kulcs?	
Mi a helyi kulcsszerver azonosítója?	
Mi a helyi adatvégpont azonosítója?	
Mi a távoli kulcsszerver azonosítója?	
Mi a távoli adatvégpont azonosítója?	
Milyen biztonságot és rendszerteljesítményt követel meg az adatok védelméhez? • Legnagyobb biztonság, legkisebb teljesítmény • Kiegyensúlyozott biztonság és teljesítmény • Legkisebb biztonság, legnagyobb teljesítmény	

Kézi kapcsolatok tervezési munkalapja

Ezt a munkalapot használja fel segítségül olyan VPN kapcsolatok létrehozásához, amelyek a kulcskezeléshez nem használják az IKE protokollt.

A VPN beállításának megkezdése előtt minden kérdést válaszoljon meg:

Előfeltétel ellenőrzőlista	**Válaszok**
Az OS/400 (5722-SS1) kiadása V5R2 vagy újabb?	
A Digitális igazolás kezelő (5722-SS1, 34. opció) telepítve van?	
Van telepített Cryptographic Access Provider (5722-AC2 vagy AC3) termék?	
Telepítve van az iSeries Access for Windows (5722-XE1) termék?	
Telepítve van az iSeries navigátor?	
Telepítve van az iSeries navigátor Hálózat részösszetevője?	
Telepítve van a TCP/IP Connectivity Utilities for OS/400 (5722-TC1) termék?	
Beállította a Szerver biztonsági adatok megtartása (QRETSVRSEC *SEC) rendszerváltozót 1-re?	
Be van állítva a TCP/IP az iSeries szerveren (beleértve az IP csatolókat, útvonalakat, a helyi hosztnevet és a helyi tartománynevet)?	
A szokásos TCP/IP kommunikáció működik a szükséges végpontok között?	
Alkalmazta a legújabb ideiglenes program javításokat (PTF)?	
Ha a VPN alagút forgalma tűzfalakon vagy IP csomagszűrést megvalósító útválasztókon halad át, akkor támogatja a tűzfal vagy útválasztó az AH és ESP protokollokat?	
A tűzfalak vagy útválasztók be vannak állítva az AH és ESP protokollok engedélyezésére?	
A tűzfalakon be van állítva az IP továbbítás?	

A kézi VPN kapcsolat beállításához szükséges információk	Válaszok
Milyen típusú kapcsolatot hoz létre? • Hoszt-hoszt • Hoszt-átjáró • Átjáró-hoszt • Átjáró-átjáró	
Mi lesz a kapcsolat neve?	
Mi a helyi kapcsolati végpont azonosítója?	
Mi a távoli kapcsolati végpont azonosítója?	
Mi a helyi adatvégpont azonosítója?	
Mi a távoli adatvégpont azonosítója?	
Milyen típusú forgalmat (helyi port, távoli port és protokoll) tervez engedélyezni a kapcsolatban?	
Kíván címfordítást használni a kapcsolatban? További információkat a Hálózati cím fordítás VPN kapcsolatokban című témakörben talál.	
Alagút vagy szállítási módot fog használni?	
Milyen IPSec protokollt fog használni a kapcsolat (AH, ESP vagy AH és ESP)? További információkat az IP biztonság (IPSec) című témakörben talál.	
Milyen hitelesítési algoritmust fog alkalmazni a kapcsolat (HMAC-MD5 vagy HMAC-SHA)?	
Milyen titkosítási algoritmust fog alkalmazni a kapcsolat (DES-CBC vagy 3DES-CBC)? **Megjegyzés:** Titkosítási algoritmus csak akkor választható, ha kiválasztotta az ESP IPSec protokollt.	
Mi az AH bejövő kulcsa? MD5 használatakor a kulcs egy 16 byte-os hexadecimális karaktersorozat. SHA használata esetén a kulcs egy 20 byte-os hexadecimális karaktersorozat. A bejövő kulcsnak pontosan meg kell egyeznie a távoli szerver kimenő kulcsával.	
Mi az AH kimenő kulcsa? MD5 használatakor a kulcs egy 16 byte-os hexadecimális karaktersorozat. SHA használata esetén a kulcs egy 20 byte-os hexadecimális karaktersorozat. A kimenő kulcsnak pontosan meg kell egyeznie a távoli szerver bejövő kulcsával.	
Mi az ESP bejövő kulcsa? DES használata esetén a kulcs egy 8 byte-os hexadecimális karaktersorozat. 3DES használata esetén a kulcs egy 24 byte-os hexadecimális karaktersorozat. A bejövő kulcsnak pontosan meg kell egyeznie a távoli szerver kimenő kulcsával.	
Mi az ESP kimenő kulcsa? DES használata esetén a kulcs egy 8 byte-os hexadecimális karaktersorozat. 3DES használata esetén a kulcs egy 24 byte-os hexadecimális karaktersorozat. A kimenő kulcsnak pontosan meg kell egyeznie a távoli szerver bejövő kulcsával.	
Mi a bejövő biztonsági paraméterindex (SPI)? A bejövő SPI egy 4 byte-os hexadecimális karaktersorozat, amelyben az első byte értéke 00. A bejövő SPI értéknek pontosan meg kell egyeznie a távoli szerver kimenő SPI értékével.	

A kézi VPN kapcsolat beállításához szükséges információk	Válaszok
Mi a kimenő SPI? A kimenő SPI egy 4 byte-os hexadecimális karaktersorozat. A kimenő SPI értéknek pontosan meg kell egyeznie a távoli szerver bejövő SPI értékével.	

VPN beállítása

A VPN felület több lehetőséget is biztosít a VPN kapcsolatok beállítására. A beállítandó kapcsolattípus eldöntéséhez és a beállítás módjának leírásához folytassa az olvasást.

Beállítandó kapcsolat típusa
A **dinamikus** kapcsolatok az Internet kulcscsere (IKE) protokoll felhasználásával dinamikusan állítják elő és egyeztetik a kapcsolat biztonságát nyújtó kulcsokat. A dinamikus kapcsolatok kiemelkedő szintű biztonságot jelentenek a rajtuk áthaladó adatok számára, mivel a kulcsok rendszeres időközönként automatikusan cserélődnek. Következésképp ha egy támadó meg is szerez egy kulcsot, nem lesz ideje a megtörésére, és a kulcs által védett forgalom visszafejtésére.

A **kézi (Lásd: 37)** kapcsolatok nem támogatják az IKE egyeztetéseket, vagyis az automatikus kulcskezelést. Továbbá a jellemzők nagy részének pontosan meg kell egyeznie a kapcsolat két végpontján. A kézi kapcsolatok által használt statikus kulcsok nem kerülnek frissítésre vagy módosításra a kapcsolat közben. A kézi kapcsolatokat le kell állítani a hozzájuk tartozó kulcs módosításához. Ha ezt biztonsági kockázatként értékeli, akkor helyettük hozzon létre inkább dinamikus kapcsolatokat.

Dinamikus VPN kapcsolatok beállítása
A VPN valójában a kapcsolat jellemzőit leíró konfigurációs objektumok csoportja. A dinamikus VPN kapcsolatoknak szüksége van mindeme objektumokra a megfelelő működéshez. Az egyes VPN konfigurációs objektumok beállításával kapcsolatban nézze meg a következő témaköröket:

> **Tipp:**
> **Kapcsolatok beállítása az Új kapcsolat varázslóval**
> A dinamikus kapcsolatok létrehozására általában a Kapcsolat varázslót kell használni. A varázsló automatikusan létrehozza a VPN megfelelő működéséhez szükséges valamennyi konfigurációs objektumot, beleértve a csomagszabályokat is. Ha megadja a varázslónak a VPN csomagszabályok aktiválását, akkor az alábbi *Kapcsolat indítása* lépést kihagyhatja. Ellenkező esetben a varázsló befejeződése után aktiválnia kell a csomagszabályokat, és csak ezután indíthatja el a kapcsolatot.

Ha úgy dönt, hogy a dinamikus VPN kapcsolatok létrehozására nem a varázslót használja, akkor konfiguráció létrehozásához tegye a következőket:

1. **VPN biztonsági stratégiák beállítása**
   Be kell állítani az összes dinamikus kapcsolatra vonatkozó VPN biztonsági stratégiát. Ez az Internet kulcscsere stratégia és adat stratégia írja elő, hogyan védi az IKE az egyeztetés 1. és 2. fázisát.
2. **Biztonságos kapcsolatok beállítása**
   A kapcsolat biztonsági stratégiáinak meghatározása után kell beállítani magát a biztonságos kapcsolatot. Dinamikus kapcsolatoknál a biztonságos kapcsolati objektum egy dinamikus kulcsú csoportból és egy dinamikus kulcsú kapcsolatból áll. A **dinamikus kulcsú csoport** adja meg egy vagy több VPN kapcsolat között jellemzőit, míg a **dinamikus kulcsú kapcsolat** határozza meg a végpont párok között felépített egyedi adatkapcsolatok jellemzőit. A dinamikus kulcsú kapcsolat a dinamikus kulcsú csoportban található.

   Megjegyzés: A következő két lépést (*Csomagszabályok beállítása* és a *Szabályok csatolójának meghatározása*) csak akkor kell végrehajtani, ha a VPN felület **Dinamikus kulcsú csoport - Kapcsolatok** lapján kiválasztja a **Stratégia szűrőszabály meghatározására a Csomagszabályokban kerül sor** beállítást. Ellenkező esetben a szabályok a VPN konfiguráció részeként jönnek létre, és kerülnek alkalmazásra a megadott csatolóra.

Ajánlott, hogy a stratégia szűrőszabályokat mindig a VPN felület állítsa elő. Ehhez a **Dinamikus kulcsú csoport - Kapcsolatok** lapon az **Alábbi stratégia szűrő előállítása a csoporthoz** beállítást kell kiválasztani.

3. **Csomagszabályok beállítása**
   A VPN konfigurálásának befejezése után létre kell hozni és alkalmazni kell a kapcsolat adatforgalmát engedélyező szűrőszabályokat. A **IPSec előtti** szabályok minden IKE forgalmat engedélyeznek a megadott csatolókon, így az IKE elvégezheti a kapcsolatok egyeztetését. A **stratégia szűrő**szabály határozza meg, hogy a társított új dinamikus kulcsú csoportot milyen címek, protokollok és portok használhatják.

   V4R4 vagy V4R5 kiadásról végzett áttérés során ha rendelkezik VPN kapcsolatokkal és az aktuális kiadásban továbbra is használni kívánt stratégia szűrőkkel, akkor a régi és az új stratégia szűrők megfelelő együttműködésének biztosításáról olvassa el a *Stratégia szűrőszabályok átvétele az aktuális kiadásra* című témakört.
4. **Csatoló meghatározása a szabályokhoz**
   A csomagszabályok és a a VPN kapcsolat működéséhez szükséges további szabályok beállítása után meg kell adni, hogy ezek a szabályok melyik csatolóra vonatkozzanak.
5. **Csomagszabályok aktiválása**
   Miután meghatározta a csomagszabályok csatolóját, aktiválni kell őket a kapcsolat indítása előtt.
6. **Kapcsolat indítása**
   Ezzel a feladattal indíthatja el a kapcsolatokat.

Kézi VPN kapcsolatok beállítása

Mint azt a neve is sugallja, a kézi kapcsolatok valamennyi tulajdonságát, beleértve a bejövő és kimenő kulcsokat is, egyenként be kell állítani. A kézi kapcsolatok beállításával kapcsolatban nézze meg a következő témaköröket:

1. **Kézi kapcsolatok beállítása**
   A kézi kapcsolatok határozzák meg egy kapcsolat jellemzőit, beleértve a használt biztonsági protokollokat, illetve a kapcsolati- és adatvégpontokat.

   Megjegyzés: A következő két lépést (*Stratégia szűrőszabályok beállítása* és a *Szabályok csatolójának meghatározása*) csak akkor kell végrehajtani, ha a VPN felület **Kézi kapcsolat - Kapcsolatok** lapján kiválasztja a **Stratégia szűrőszabály meghatározására a Csomagszabályokban kerül sor** beállítást. Ellenkező esetben a szabályok a VPN konfiguráció részeként jönnek létre.

   Ajánlott, hogy a stratégia szűrőszabályokat mindig a VPN felület állítsa elő. Ehhez válassza ki a **Kézi kapcsolat - Kapcsolatok** lap **Adatvégpontoknak megfelelő stratégia szűrő előállítása** beállítását.
2. **Stratégia szűrőszabályok beállítása**
   A kézi kapcsolat jellemzőinek meghatározása után létre kell hozni és alkalmazni kell a kapcsolat adatforgalmát engedélyező szűrőszabályokat. A **stratégia szűrő**szabály határozza meg, hogy a társított kapcsolatot milyen címek, protokollok és portok használhatják.
3. **Csatoló meghatározása a szabályokhoz**
   A csomagszabályok és a a VPN kapcsolat működéséhez szükséges további szabályok beállítása után meg kell adni, hogy ezek a szabályok melyik csatolóra vonatkozzanak.
4. **Csomagszabályok aktiválása**
   Miután meghatározta a csomagszabályok csatolóját, aktiválni kell őket a kapcsolat indítása előtt.
5. **Kapcsolat indítása**
   Ezzel a feladattal indíthatja el a helyi kezdeményezésű kapcsolatokat.

VPN kapcsolatok beállítása az Új kapcsolat varázslóval

Az Új kapcsolat varázsló lehetővé teszi hosztok és átjárók tetszőleges kombinációja között kialakított virtuális magánhálózatok (VPN) létrehozását. Ilyen például a hoszt-hoszt, átjáró-hoszt, hoszt-átjáró és az átjáró-átjáró.

A varázsló automatikusan létrehozza a VPN megfelelő működéséhez szükséges valamennyi konfigurációs objektumot, beleértve a csomagszabályokat is. Ha azonban további funkciókkal, például naplózással vagy hálózati cím fordítással (VPN NAT) kívánja kiegészíteni a VPN kapcsolatot, akkor elképzelhető, hogy szükség lesz a kapcsolat beállításainak kézi pontosítására, amelyet a megfelelő dinamikus kulcsú csoport vagy kapcsolat adatlapjain végezhet el. Ehhez először le kell állítani a kapcsolatot, amennyiben az aktív. Ezután kattintson a jobb egérgombbal a dinamikus kulcsú csoportra vagy kapcsolatra, majd válassza az előugró menü **Tulajdonságok** menüpontját.

A kezdés előtt konzultáljon a VPN tervezési tanácsadóval. A tanácsadó lehetőséget nyújt arra, hogy a fontos információkat még a VPN létrehozása előtt összegyűjtse.

VPN létrehozásához az Kapcsolat varázslóban tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Új kapcsolat** menüpontját a varázsló indításához.
3. Kövesse a varázsló útmutatásait egy alapszintű VPN konfiguráció létrehozásához. Ha segítségre van szüksége, akkor kattintson a **Súgó** gombra.

VPN biztonsági stratégiák beállítása

Miután meghatározta a VPN felhasználásának módját, be kell állítani a VPN biztonsági stratégiákat. Ez pontosabban a következő tevékenységből áll:

- **Internet kulcscsere (IKE) stratégia beállítása**
  Az IKE stratégia határozza meg, hogy az IKE milyen szintű hitelesítést és titkosítást alkalmaz az egyeztetés 1. fázisában. Az IKE 1. fázisa alakítja ki az ezt követő 2. egyeztetési fázisban küldött üzenetek védelmére szolgáló kulcsokat. Kézi kapcsolatok létrehozásakor IKE stratégia meghatározására nincs szükség. Ha a VPN-t az Új kapcsolat varázslóval hozza létre, akkor a varázsló létrehozhatja az IKE stratégiát is.
- **Adat stratégia beállítása**
  Az adat stratégia határozza meg a VPN kapcsolatban forgalmazott adatokat milyen szintű hitelesítés és titkosítás védi. Az egymással kommunikáló rendszerek ezekben a jellemzőkben az Internet kulcscsere (IKE) 2. egyeztetési fázisa során egyeznek meg. Kézi kapcsolatok létrehozásakor adat stratégia meghatározására nincs szükség. Ha a VPN-t az Új kapcsolat varázslóval hozza létre, akkor a varázsló létrehozhatja az adat stratégiát is.

A VPN biztonsági stratégiák konfigurálásának befejezése után be kell állítani a védett kapcsolatokat.

Internet kulcscsere (IKE) stratégia beállítása

Az IKE stratégiák határozzák meg, hogy az IKE milyen szintű hitelesítést és titkosítást alkalmaz az egyeztetés 1. fázisában. Az IKE 1. fázisa alakítja ki az ezt követő 2. egyeztetési fázisban küldött üzenetek védelmére szolgáló kulcsokat. A VPN RSA aláírást vagy előzetesen megosztott kulcsot használ az egyeztetés 1. fázisának védelmére. Ha a kulcsszerverek azonosítására digitális igazolásokat kíván használni, akkor ezeket először be kell állítani a Digitális igazolás kezelőben (5722-SS1 34. opció). Az IKE stratégia azt is meghatározza, hogy a stratégiát melyik távoli kulcsszerver használja.

Új IKE stratégia meghatározásához vagy meglévő módosításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> IP biztonsági stratégiák** elemeket.
2. Új stratégia létrehozásához kattintson a jobb egérgombbal az **Internet kulcscsere stratégiák** elemre, majd válassza az előugró menü **Új Internet kulcscsere stratégia** menüpontját. Meglévő stratégia módosításához a bal oldali ablakrészben kattintson az **Internet kulcscsere stratégiák** elemre, ezután a jobb oldali ablakrészben kattintson a jobb egérgombbal a módosítani kívánt stratégiára, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Töltsön ki minden adatlapot. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.

4. Kattintson az **OK** gombra a változások mentéséhez.

Adat stratégiák beállítása

Az adat stratégia határozza meg a VPN kapcsolatban forgalmazott adatokat milyen szintű hitelesítés és titkosítás védi. Az egymással kommunikáló rendszerek ezekben a jellemzőkben az Internet kulcscsere (IKE) protokoll 2. egyeztetési fázisa során egyeznek meg.

Új adat stratégia meghatározásához vagy meglévő módosításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> IP biztonsági stratégiák** elemeket.
2. Új adat stratégia létrehozásához kattintson a jobb egérgombbal az **Adat stratégiák** bejegyzésre, majd válassza az előugró menü **Új adat stratégia** menüpontját. Meglévő adat stratégia módosításához kattintson a bal oldali ablaktábla **Adat stratégiák** elemére, ezután a jobb oldali ablaktáblán kattintson a jobb egérgombbal a módosítani kívánt adat stratégián, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Töltsön ki minden adatlapot. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
4. Kattintson az **OK** gombra a változások mentéséhez.

VPN biztonságos kapcsolat beállítása

A kapcsolat biztonsági stratégiáinak meghatározása után kell beállítani magát a biztonságos kapcsolatot. Dinamikus kapcsolatoknál a biztonságos kapcsolati objektum egy dinamikus kulcsú csoportból és egy dinamikus kulcsú kapcsolatból áll.

A **dinamikus kulcsú csoport** adja meg egy vagy több VPN kapcsolat között jellemzőit. A dinamikus kulcsú csoportok beállításakor lehetőség van arra, hogy a csoport kapcsolatai azonos stratégiákat használjanak eltérő adatvégpontokhoz. A dinamikus kulcsú csoportok emellett lehetővé teszik a sikeres egyeztetést a távoli kezdeményezőkkel az olyan esetekben, amikor a távoli rendszer által felajánlott adatvégpontok előzetesen nem pontosan ismertek. Ez úgy történik, hogy a rendszer a dinamikus kulcsú csoport stratégia információihoz társít egy IPSEC tevékenységtípust meghatározó stratégia szűrőszabályt. Ha a távoli kezdeményező által felajánlott adatvégpontok beleesnek az IPSEC szűrőszabály által megadott tartományba, akkor a dinamikus kulcsú csoportban meghatározott stratégia alkalmazható az adatvégpontra.

A **dinamikus kulcsú kapcsolat** határozza meg a végpont párok között felépített egyedi adatkapcsolatok jellemzőit. A dinamikus kulcsú kapcsolat a dinamikus kulcsú csoportban található. Miután egy dinamikus kulcsú csoport létrehozásával megadta a csoport kapcsolatai által használandó stratégiákat, létrehozhatja a helyi kezdeményezésű csatlakozások egyéni dinamikus kulcsú kapcsolatait.

Védett kapcsolati objektum beállításához tegye a következőket:

1. rész - Dinamikus kulcsú csoport beállítása

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a jobb egérgombbal a **Csoportonként** elemre, majd válassza az előugró menü **Új dinamikus kulcsú csoport** menüpontját.
3. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
4. Kattintson az **OK** gombra a változások mentéséhez.

2. rész - Dinamikus kulcsú kapcsolat beállítása

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok —> Csoportonként** elemeket.

2. Az iSeries navigátor bal oldali ablaktábláján kattintson a jobb egérgombbal az első részben létrehozott dinamikus kulcsú csoportra, majd válassza az előugró menü **Új dinamikus kulcsú kapcsolat** menüpontját.
3. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
4. Kattintson az **OK** gombra a változások mentéséhez.

A fenti lépések befejezése után aktiválni kell a kapcsolat megfelelő működéséhez szükséges csomagszabályokat.

Megjegyzés: A legtöbb esetben engedélyezni kell a VPN felület számára a VPN csomagszabályok automatikus előállítását a **Dinamikus kulcsú csoport - Kapcsolatok** lap **Alábbi stratégia szűrő előállítása a csoporthoz** beállításának kiválasztásával. Ha a **Stratégia szűrőszabály meghatározására a Csomagszabályokban kerül sor** beállítást választja, akkor a Csomagszabály szerkesztővel be kell állítani a VPN csomagszabályokat, majd aktiválni kell azokat.

Kézi kapcsolatok beállítása

Mint azt a neve is sugallja, a kézi kapcsolatok valamennyi tulajdonságát egyenként be kell állítani. Továbbá a beállítások nagy részének *pontosan* meg kell egyeznie a kapcsolat két végpontján. Például a bejövő kulcsoknak meg kell egyezniük a távoli rendszeren beállított kimenő kulcsoknak, máskülönben a kapcsolat nem építhető fel.

A kézi kapcsolatok által használt statikus kulcsok nem kerülnek frissítésre vagy módosításra a kapcsolat közben. A kézi kapcsolatokat le kell állítani a hozzájuk tartozó kulcs módosításához. Ha úgy gondolja, hogy ez biztonsági kockázat, és a kapcsolat mindkét végpontja támogatja az Internet kulcscsere (IKE) protokoll használatát, akkor kézi kapcsolatok helyett érdemes megfontolni dinamikus kulcsú kapcsolatok beállítását.

Kézi kapcsolat tulajdonságainak meghatározásához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a jobb egérgombbal a **Minden kapcsolat** bejegyzésre, majd válassza az előugró menü **Új kézi kapcsolat** menüpontját.
3. Töltsön ki minden adatlapot. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
4. Kattintson az **OK** gombra a változások mentéséhez.

Megjegyzés: A legtöbb esetben engedélyezni kell a VPN felület számára a VPN csomagszabályok automatikus előállítását a **Kézi kapcsolat - Kapcsolatok** lap **Adatvégpontoknak megfelelő stratégia szűrő előállítása** beállításának kiválasztásával. Ha a **Stratégia szűrőszabály meghatározására a Csomagszabályokban kerül sor** beállítást választja, akkor saját kezűleg be kell állítani a stratégia szűrőszabályokat, majd aktiválni kell azokat.

VPN csomagszabályok beállítása

Ha első alkalommal állít be kapcsolatot, akkor ajánlott engedélyezni a VPN felület számára a VPN csomagszabályok automatikus előállítását. Ez az Új kapcsolat varázsló és a VPN adatlapok használatakor is megteheti.

Ha úgy dönt, hogy saját VPN csomagszabályokat hoz létre az iSeries navigátor Csomagszabály szerkesztőjével, akkor az esetleges további szabályokat is létre kell hozni. Ellenben ha a stratégia szűrőszabályokat a VPN állítja elő, akkor minden további stratégia szűrőszabályt ily módon kell létrehozni.

A VPN kapcsolatok általában kétféle szűrőszabályt igényelnek: IPSec előtti szabályokat és stratégia szűrőszabályokat. A szabályoknak az iSeries navigátor Csomagszabály szerkesztőjében végzett

beállításáról további információkhoz az alábbi témakörökből juthat. Ha további részletek is érdeklik a VPN és a szűrés viszonyáról, akkor nézze meg a VPN alapelvek rész *VPN és IP szűrés* című témakörét.

- **IPSec előtti szabályok**
  Az IPSec előtti szabályok azok, amelyek az IPSEC tevékenységtípust meghatározó szabályok előtt kerülnek betöltésre. A témakör csak a VPN megfelelő működéséhez szükséges IPSec előtti szabályokkal foglalkozik. Ebben az esetben az IPSec előtti szabályok kimerülnek egy olyan szabálypárban, amely engedélyezi az IKE feldolgozást a kapcsolatban. Az IKE biztosítja a kapcsolatokban a kulcsok dinamikus előállítását és egyeztetését. Az adott hálózati környezettől és a biztonsági stratégiától függően további IPSec előtti szabályok hozzáadására is szükség lehet.

  Megjegyzés: Ilyen jellegű IPSec előtti szabály beállítása csak abban az esetben szükséges, ha már rendelkezik IKE forgalmat engedélyező más szabályokkal bizonyos rendszerek számára. Ha a rendszeren nincsenek kifejezetten az IKE forgalom engedélyezését szolgáló szűrőszabályok, akkor az IKE forgalom hallgatólagosan megengedett.
- **Stratégia szűrőszabály**
  A stratégia szűrőszabály határozza meg a VPN kapcsolatban engedélyezett forgalmat és a forgalomra alkalmazott adatvédelmi stratégiát.

Kezdés előtt megfontolandó tényezők
Ha szűrőszabályokat ad hozzá egy csatolóhoz, akkor a rendszer automatikusan hozzáad a vonalhoz egy alapértelmezett DENY szabályt. Ez azt jelenti, hogy ami nincs kifejezetten engedélyezve, az tiltott. Ez a szabály nem jeleníthető meg, és nem is módosítható. Ennek eredményeképpen úgy találhatja, hogy korábban működő kapcsolatok titokzatos módon nem működnek a VPN szűrőszabályok aktiválása után. Ha a csatolón a virtuális magánhálózaton kívül más forgalmat is engedélyezni kíván, akkor ehhez fel kell venni egy kifejezett PERMIT szabályt.

A megfelelő szűrőszabályok beállítása után meg kell adni a csatolót, amelyre alkalmazni kívánja a szabályokat, majd aktiválni kell azokat.

A szűrőszabályok pontos beállítása rendkívül fontos. Ennek elmulasztásakor a szűrőszabályok az iSeries szerver teljes kimenő és bejövő forgalmát letilthatják. Ebbe a szűrőszabályok beállítására használt iSeries navigátor kapcsolat is beletartozik.

Ha a szűrőszabályok nem engedélyezik az iSeries navigátor forgalmát, akkor az iSeries navigátor nem fog tudni kommunikálni az iSeries szerverrel. Ha ilyen helyzetbe hozza magát, akkor az iSeries szerverre be kell jelentkezni egy olyan csatolón keresztül, amelynek csatlakozása biztosított, ilyen például a Műveleti konzol kapcsolat. A rendszer összes szűrőjének eltávolításához használja a RMVTCPTBL parancsot. A parancs leállítja és újraindítja az összes *VPN szervert is. Ha erre sor került, akkor állítsa be a szűrőket, és aktiválja azokat ismét.

IPSec előtti szűrőszabályok beállítása
Figyelem: Ezt a feladatot csak akkor kell elvégezni, ha megadta, hogy a VPN ne állítsa elő automatikusan a stratégia szűrőszabályokat.

Két Internet kulcscsere (IKE) szerver dinamikusan egyezteti és frissíti a kulcsokat. Az IKE a közismert 500-as portot használja. Az IKE megfelelő működésének biztosításához engedélyezni kell az UDP forgalmat az 500-as porton. Ehhez két szűrőszabályt kell létrehozni, egyet a bejövő forgalomhoz, egyet pedig a kimenőhöz, ezekkel a kapcsolat képes a védelmét szolgáló kulcsok dinamikus egyeztetésére.

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomag szabályok** elemen, majd válassza az előugró menü **Szabályszerkesztő** menüpontját. Megjelenik a Csomagszabály szerkesztő, amelyben létrehozhatja és szerkesztheti az iSeries szerver szűrő- és NAT szabályait.
3. Az Üdvözlet párbeszédablakban válassza az **Új csomagszabály fájl létrehozása** lehetőséget, majd kattintson az **OK** gombra.
4. A Csomagszabály szerkesztően válassza a **Beszúrás —> Szűrő** menüpontot.

5. Az **Általános** lapon adjon nevet a VPN szűrőszabály készletnek. Legalább három különböző készlet létrehozása ajánlott: egy az IPSec előtt szűrőszabályoknak, egy a stratégia szűrőszabályoknak, egy pedig az egyéb PERMIT és DENY szűrőszabályoknak. Az IPSec előtti szűrőszabályokat tartalmazó készlet nevének a *PREIPSEC* előtaggal kell rendelkeznie. Például PREIPSEC_SZŰRŐK.
6. A **Tevékenység** mezőben válassza ki a legördülő lista **PERMIT** elemét.
7. Az **Irány** mezőben válassza ki a legördülő lista **OUTBOUND** elemét.
8. A **Forráscím neve** mezőben válassza ki az első legördülő lista **=** bejegyzését, majd írja be a helyi kulcsszerver IP címét a másik mezőbe. A helyi kulcsszerver IP címét az IKE stratégiában adta meg.
9. A **Célcím neve** mezőben válassza ki az első legördülő lista **=** bejegyzését, majd írja be a távoli kulcsszerver IP címét a másik mezőbe. A távoli kulcsszerver IP címét az IKE stratégiában is megadta.
10. A **Szolgáltatások** lapon válassza ki a **Szolgáltatás** választógombot. Ez engedélyezi a **Protokoll**, a **Forrásport** és a **Célport** mezőket.
11. A **Protokoll** mezőben válassza ki az **UDP** protokollt a legördülő listából.
12. A **Forrásport** mezőben válassza ki az egyenlőségjelet, a második mezőbe írjon be 500-at.
13. Ismételje meg az előző lépést a **Célport** esetében is.
14. Kattintson az **OK** gombra.
15. Ismételje meg a fenti lépéseket az INBOUND szűrő létrehozásához. Használjon azonos készletnevet, a címeket pedig értelemszerűen cserélje fel.

Megjegyzés: az IKE forgalom engedélyezésére van egy egyszerűbb bár kevésbé biztonságos másik módszer is. Ilyenkor csak egy IPSec előtti szűrő kerül létrehozásra, az **Irány**, a **Forráscím neve** és a **Célcím neve** mezőkbe pedig helyettesítő karakter (*) kerül.

A következő lépés a VPN által védett IP forgalmat meghatározó stratégia szűrőszabály beállítása.

Stratégia szűrőszabályok beállítása

Figyelem: Ezt a feladatot csak akkor kell elvégezni, ha megadta, hogy a VPN ne állítsa elő automatikusan a stratégia szűrőszabályokat.

A stratégia szűrőszabály (IPSEC tevékenységet meghatározó szabály) határozza meg, hogy a VPN kapcsolatot milyen címek, protokollok és portok használhatják. Ez határozza meg a VPN kapcsolat forgalmára alkalmazott stratégiát is. Stratégia szűrőszabály konfigurálásához tegye a következőket:

Megjegyzés: Ha épp most állította be a dinamikus kapcsolatok IPSec előtti szabályait, akkor a Csomagszabály szerkesztőnek még mindig nyitva kell lennie. Ebben az esetben folytassa a 4. lépésnél.

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomag szabályok** elemen, majd válassza az előugró menü **Szabályszerkesztő** menüpontját. Megjelenik a Csomagszabály szerkesztő, amelyben létrehozhatja és szerkesztheti az iSeries szerver szűrő- és NAT szabályait.
3. Az Üdvözlet párbeszédablakban válassza az **Új csomagszabály fájl létrehozása** lehetőséget, majd kattintson az **OK** gombra.
4. A Csomagszabály szerkesztően válassza a **Beszúrás —> Szűrő** menüpontot.
5. Az **Általános** lapon adjon nevet a VPN szűrőszabály készletnek. Legalább három különböző készlet létrehozása ajánlott: egy az IPSec előtt szűrőszabályoknak, egy a stratégia szűrőszabályoknak, egy pedig az egyéb PERMIT és DENY szűrőszabályoknak. Például STRATÉGIA_SZŰRŐK.
6. A **Tevékenység** mezőben válassza ki a legördülő lista **IPSEC** elemét. Az **Irány** mező felveszi az alapértelmezett OUTBOUND értéket, amely nem is módosítható. Bár a mező alapértelmezett értéke OUTBOUND, valójában kétirányú. Az OUTBOUND a bemeneti értékek értelmezésének tisztázása érdekében jelenik meg. Például a forrásértékek helyi értékek, a cél értékek távoli értékek.
7. A **Forráscím nevénél** az első mezőben válassza ki az egyenlőségjelet, a második mezőben pedig adja meg a helyi adatvégpont IP címét. Lehetőség van IP címtartomány vagy IP cím és alhálózati maszk megadására is, amennyiben ezeket előzőleg beállította a **Címek meghatározása** funkcióval.

8. A **Célcím nevénél** az első mezőben válassza ki az egyenlőségjelet, a második mezőben pedig adja meg a távoli adatvégpont IP címét. Lehetőség van IP címtartomány vagy IP cím és alhálózati maszk megadására is, amennyiben ezeket előzőleg beállította a **Címek meghatározása** funkcióval.
9. A **Naplózás** mezőben adja meg a szükséges naplózási szintet.
10. A **Kapcsolat neve** mezőben válassza ki, melyik kapcsolatmeghatározásra vonatkoznak a szűrőszabályok.
11. Adjon meg egy leírást. (nem kötelező)
12. A **Szolgáltatások** lapon válassza ki a **Szolgáltatás** választógombot. Ez engedélyezi a **Protokoll**, a **Forrásport** és a **Célport** mezőket.
13. A **Protokoll**, a **Forrásport** és a **Célport** mezőkben írja be a forgalomnak megfelelő értékeket. Kiválaszthatja a legördülő lista csillag (*) elemét is. Ez lehetővé teszi, hogy a VPN tetszőleges portot és protokollt használjon.
14. Kattintson az **OK** gombra.

A következő lépés a csatoló meghatározása, amelyre a szűrőszabályok vonatkozni fognak.

Megjegyzés: Amikor szűrőszabályokat ad hozzá egy csatolóhoz, akkor a rendszer automatikusan hozzáad a csatolóhoz egy alapértelmezett DENY szabályt is. Ez azt jelenti, hogy ami nincs kifejezetten engedélyezve, az tiltott. Ez a szabály nem jeleníthető meg, és nem is módosítható. Ennek eredményeképpen úgy találhatja, hogy korábban működő kapcsolatok érdekes módon nem működnek a VPN csomagszabályok aktiválása után. Ha a csatolón a virtuális magánhálózaton kívül más forgalmat is engedélyezni kíván, akkor ehhez fel kell venni egy kifejezett PERMIT szabályt.

VPN szűrőszabályok csatolójának meghatározása

A VPN csomagszabályok és a a VPN kapcsolat működéséhez szükséges további szabályok beállítása után meg kell adni, melyik csatolóra vonatkozzanak ezek a szabályok.

A VPN szűrőszabályok alkalmazási csatolójának meghatározásához tegye a következőket:

Megjegyzés: Ha épp most állította be a VPN csomagszabályokat, akkor a Csomagszabályok felületnek még nyitva kell lennie. Ebben az esetben folytassa a 4. lépésnél.

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomag szabályok** elemen, majd válassza az előugró menü **Szabályszerkesztő** menüpontját. Megjelenik a Csomagszabály szerkesztő, amelyben létrehozhatja és szerkesztheti az iSeries szerver szűrő- és NAT szabályait.
3. Az Üdvözlet párbeszédablakban válassza az **Új csomagszabály fájl létrehozása** lehetőséget, majd kattintson az **OK** gombra.
4. A Csomagszabály szerkesztően válassza a **Beszúrás —> Szűrő csatoló** menüpontot.
5. Az **Általános** lapon jelölje ki a **Vonalnév** beállítást, majd a legördülő listából válassza ki, hogy melyik vonalleírásra kívánja alkalmazni a VPN csomagszabályokat.
6. Adjon meg egy leírást. (nem kötelező)
7. A **Szűrőkészletek** lapon kattintson a **Hozzáadás** gombra a beállított szűrők mindegyikének hozzáadásához.
8. Kattintson az **OK** gombra.
9. Mentse a szabályfájlt. A fájl az iSeries integrált fájlrendszerén kerül mentésre .I3P kiterjesztéssel. **Megjegyzés:** Ne mentse a fájlt az alábbi katalógusba:

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

   Ez a katalógus a rendszer számára van fenntartva. Ha a csomagszabályok leállításához valaha is szüksége lesz a RMVTCPTBL *ALL parancsra, akkor az a fenti katalógus összes fájlját törli.

Miután meghatározta a szűrőszabályok csatolóját, aktiválni kell őket a VPN indítása előtt.

VPN csomagszabályok aktiválása

A VPN csomagszabályokat aktiválni kell, mielőtt a VPN kapcsolatokat el lehetne indítani. Csomagszabályok aktiválása (és leállítása) nem végezhető, ha a rendszeren vannak futó VPN kapcsolatok. Ennek megfelelően a VPN szűrőszabályok aktiválása előtt győződjön meg róla, hogy az érintett csatolókon nincsenek aktív kapcsolatok.

Ha a VPN kapcsolatokat az Új kapcsolat varázslóval hozza létre, akkor megadhatja a társított szűrők automatikus aktiválását. Ne feledje azonban, hogy ha a megadott csatolók bármelyikén vannak más aktív csomagszabályok is, akkor a VPN stratégia szűrőszabályok lecserélik ezeket.

» Ha a VPN által előállított szabályokat valamilyen oknál fogva a Csomagszabály szerkesztőből kívánja aktiválni, akkor tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomagszabályok** elemre, majd válassza az előugró menü **Aktiválás** menüpontját. Megjelenik a Csomagszabályok aktiválása párbeszédablak.
3. Válassza ki, hogy csak a VPN által előállított szabályokat vagy csak a megadott fájlban található szabályokat kívánja-e aktiválni. Megadhatja mindkét típusú szabálykészlet aktiválását is. Az utóbbi választása akkor lehet szükséges, ha rendelkezik különféle PERMIT és DENY szabályokkal, amelyeket a VPN által előállított szabályok mellett szintén érvénybe kíván léptetni a csatolón.
4. Válassza ki a csatolót, amelyen a szabályokat aktiválni kívánja. Az aktiválás történhet egy adott csatolón, pont-pont azonosítón vagy minden csatolón és pont-pont azonosítón.
5. Kattintson a párbeszédablak **OK** gombjára a szabályok ellenőrzéséhez és aktiválásához a kijelölt csatolón vagy csatolókon. Az OK gomb megnyomása után a rendszer ellenőrzi a szabályok szintaxisát, ennek eredményeit pedig a szövegszerkesztő alján található üzenet területre írja. Az adott fájlhoz és sorhoz köthető hibaüzenetek esetén kattintson a jobb egérgombbal a hibára, majd válassza az előugró menü **Ugrás sorra** menüpontját a sor kijelöléséhez. «

A szűrőszabályok aktiválása után készen áll a VPN kapcsolat elindítására.

VPN kapcsolatok indítása

A megadott útmutatások feltételezik a VPN kapcsolat megfelelő beállítását. A VPN kapcsolat indításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Ha a VPN szerver nincs elindítva, akkor kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Indítás** menüpontját. Elindul a VPN szerver.
3. Győződjön meg róla, hogy a csomagszabályok aktiválása megtörtént.
4. Bontsa ki a **Virtuális magánhálózatok —> Védett kapcsolatok** elemet.
5. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
6. Kattintson a jobb egérgombbal az elindítani kapcsolatra, majd válassza az előugró menü **Indítás** menüpontját. Több kapcsolat indításához válassza ki az összes indítani kívánt kapcsolatot, kattintson a jobb egérgombbal, majd válassza az előugró menü **Indítás** menüpontját.

VPN kezelése

Az iSeries navigátor VPN felületén az összes kezelési feladat elvégezhető, például:

- **VPN kapcsolatok indítása**
  Ezzel a feladattal indíthatja el a helyi kezdeményezésű kapcsolatokat.
- **Kapcsolatok alapértelmezett jellemzőinek beállítása**
  Az alapértelmezett értékek töltik fel az új stratégiák és kapcsolatok létrehozására szolgáló panelek mezőit. Alapértelmezések beállíthatók a biztonsági szintek, a kulcskezelés, a kulcs élettartam és a kapcsolat élettartam számára.

- **Hibás kapcsolatok alaphelyzetbe állítása**
  A hibás kapcsolatok alaphelyzetbe állítása a kapcsolatokat visszahelyezi várakozó állapotba.
- **Hibainformációk megtekintése**
  Ezzel a feladattal határozhatja meg a kapcsolatok hibáinak okát.
- **Aktív kapcsolatok jellemzőinek megjelenítése**
  Ezzel a feladattal ellenőrizheti az aktív kapcsolatok állapotát és más jellemzőit.
- **VPN szerver nyomkövetés használata**
  A VPN szerver nyomkövetés funkció lehetővé teszi a a VPN kapcsolatkezelő és VPN kulcskezelő szerverek nyomkövetéseinek beállítását, elindítását, leállítását és megjelenítését. Ez hasonló a karakteres felületen kiadott TRCTCPAPP *VPN parancshoz, azzal a különbséggel, hogy a nyomkövetés a kapcsolat aktív állapotában is megtekinthető.
- **VPN szerver munkanaplók megjelenítése**
  Ezen útmutatások felhasználásával jelenítheti meg a VPN kulcskezelő és a VPN kapcsolatkezelő munkanaplóit.
- **Kapcsolatok leállítása**
  Ezzel a feladattal állíthatja le a kapcsolatokat.
- **Biztonsági megegyezések (SA) jellemzőinek megjelenítése**
  Ezzel a feladattal tekintheti meg az engedélyezett kapcsolatokhoz társított biztonsági megegyezések (SA) jellemzőit.
- **VPN konfigurációs objektumok törlése**
  Mielőtt törölne egy VPN konfigurációs objektumot a VPN stratégia adatbázisból, legyen tisztában ennek a többi VPN kapcsolatra és kapcsolati csoportra gyakorolt hatásával.

Kapcsolatok alapértelmezett jellemzőinek beállítása

Az alapértelmezett biztonsági értékek jelennek meg a párbeszédablakok különböző mezőiben az új VPN objektumok létrehozásakor.

A VPN kapcsolatok alapértelmezett biztonsági értékinek beállításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Alapértelmezések** menüpontját.
3. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
4. Az adatlapok kitöltésének befejezése után kattintson az **OK** gombra.

Hibás kapcsolatok alaphelyzetbe állítása

Hibás állapotú kapcsolatok frissítéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a visszaállítani kívánt kapcsolatra, majd válassza az előugró menü **Alaphelyzet** menüpontját. A kapcsolat alaphelyzetbe áll és várakozás állapotba kerül. Több hibás kapcsolat egyidejű alaphelyzetbe állításához válassza ki a visszaállítani kívánt kapcsolatokat, kattintson a jobb egérgombbal, majd válassza az előugró menü **Alaphelyzet** menüpontját.

Hibainformációk megtekintése

A hibás kapcsolatokra vonatkozó információk megjelenítéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.

2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a megtekinteni kívánt hibás kapcsolatra, majd válassza az előugró menü **Hibainformációk** menüpontját.

Aktív kapcsolatok jellemzőinek megjelenítése

Az aktív vagy kérésre létrehozott kapcsolatok aktuális jellemzőinek megtekintéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a megtekinteni kívánt aktív vagy kérésre létrehozott kapcsolatra, majd válassza az előugró menü **Tulajdonságok** menüpontját.
4. A kapcsolat jellemzőinek megjelenítéséhez kattintson a **Jelenlegi attribútumok** lapra.

Az iSeries navigátor ablakban az összes kapcsolat jellemzői is megjeleníthetők. Alapértelmezésben csak az Állapot, Leírás és a Kapcsolattípus jellemzők jelennek meg. A megjelenő adatok módosításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Válassza az **Objektumok** menü **Oszlopok** menüpontját. Megjelenik egy párbeszédablak, amelyben kiválaszthatja az iSeries navigátor ablakban megjelenő jellemzőket.

A megjelenő oszlopok módosításakor tartsa szem előtt, hogy a változások nem felhasználói szintűek, hanem a teljes személyi számítógépre vonatkoznak.

VPN szerver nyomkövetés használata

A VPN szerver nyomkövetés megjelenítéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Diagnosztikai eszközök** —> **Szerver nyomkövetés** menüpontját.

A VPN kulcskezelő és a VPN kapcsolatkezelő által előállított nyomkövetés típusának meghatározásához tegye a következőket:

1. A **Virtuális magánhálózat nyomkövetés** ablakban kattintson a  (Beállítások) ikonra.
2. A **Kapcsolatkezelő** lapon adja meg a kapcsolatkezelő szerver által készített nyomkövetés típusát.
3. A **Kulcskezelő** lapon adja meg a kulcskezelő szerver által készített nyomkövetés típusát.
4. Ha a lapok kitöltése során segítségre van szüksége, akkor kattintson a **Súgó** gombra.
5. Kattintson az **OK** gombra a változások mentéséhez.
6. A nyomkövetés indításához kattintson az  (Indítás) ikonra. A legfrissebb információk megtekintéséhez időnként kattintson a  (Frissítés) ikonra.

VPN szerver munkanaplók megjelenítése

A VPN kulcskezelő vagy a VPN kapcsolatkezelő jelenlegi munkanaplóinak megjelenítéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.

2. Kattintson a jobb egérgombbal a **Virtuális magánhálózatok** elemre, majd válassza az előugró menü **Diagnosztikai eszközök**, ezután a megtekinteni kívánt szerver munkanaplónak megfelelő menüpontját.

Biztonsági megegyezések (SA) jellemzőinek megjelenítése

Az engedélyezett kapcsolatokkal társított biztonsági megegyezések (SA) jellemzőinek megjelenítéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a megfelelő aktív kapcsolatra, majd válassza az előugró menü **Biztonsági megegyezések** menüpontját. A megjelenő ablak lehetővé teszi az adott kapcsolathoz társított minden egyes SA tulajdonságainak megtekintését.

VPN kapcsolatok leállítása

Aktív vagy kérésre létrehozott kapcsolatok leállításához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a leállítani kívánt kapcsolatra, majd válassza az előugró menü **Leállítás** menüpontját. Több kapcsolat leállításához válassza ki az összes leállítani kívánt kapcsolatot, kattintson a jobb egérgombbal, majd válassza az előugró menü **Leállítás** menüpontját.

VPN konfigurációs objektumok törlése

Ha valóban szükség van a VPN stratégia adatbázis valamely VPN kapcsolatának törlésére, akkor tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Kattintson a **Minden kapcsolat** elemre a kapcsolatok listájának megjelenítéséhez a jobb oldali ablakrészben.
3. Kattintson a jobb egérgombbal a törölni kívánt kapcsolatra, majd válassza az előugró menü **Törlés** menüpontját.

VPN hibaelhárítás

A VPN összetett és gyorsan változó technológia, amely a szabványos IPSec technológiáknak legalábbis alapszintű ismeretét igényli. Járatosnak kell lennie az IP csomagszabályok terén is, mivel a VPN a megfelelő működéshez több szűrőszabályt is megkövetel. Mindezen bonyolultság miatt időről időre problémákat tapasztalat a VPN kapcsolatokkal. A VPN hibaelhárítás gyakran egyáltalán nem könnyű feladat. Sikerek eléréséhez ismernie kell a rendszert, a hálózati környezeteket, és az ezek kezelésére használt összetevőket. A VPN használata során felmerülő különféle problémák hibaelhárításához az alábbi témakörök adnak tanácsokat:

- **VPN hibaelhárítás megkezdése**
  Az itt megadottak alapján kezdheti meg a VPN kapcsolati problémák okának megkeresését és helyreállítását.
- **Általános VPN konfigurációs hibák és kijavításuk**
  Ez a témakör írja le a leggyakoribb felhasználói hibákat és ezek lehetséges kijavítását.
- **VPN hibaelhárítás a QIPFILTER napló segítségével**
  Ez a témakör nyújt további információkat a VPN szűrőszabályokkal kapcsolatban.

- **VPN hibaelhárítás a QVPN napló segítségével**
  Ez a témakör nyújt további információkat az IP forgalomról és kapcsolatokról.
- **VPN hibaelhárítás a VPN munkanaplók segítségével**
  Ez a témakör írja le a VPN által használt különféle jobok munkanaplóit.
- **VPN hibaelhárítás az OS/400 kommunikációs nyomkövetés segítségével**
  Ez a témakör írja le a kommunikációs vonalak adatainak nyomkövetését.

VPN hibaelhárítás megkezdése

A VPN problémák elemzése számtalan módon megkezdhető:

1. Mindig győződjön meg róla, hogy alkalmazta a legújabb ideiglenes program javításokat (PTF).
2. Győződjön meg róla, hogy a rendszer teljesíti a minimális VPN beállítási követelményeket.
3. Tekintse át a Hibainformációk ablakban és a VPN szerver munkanaplóiban található esetleges hibaüzeneteket a helyi és a távoli rendszeren is. A VPN kapcsolati problémák hibaelhárítása során igen gyakran ellenőriznie kell a kapcsolat mindkét végpontját. Emellett számításba kell venni, hogy négy címet kell ellenőrizni: a helyi és távoli kapcsolati végpontokat, ahol az IPSec alkalmazásra kerül az IP csomagokra, illetve a helyi és távoli adatvégpontokat, amelyek az IP csomagok forrás- és célcímei.
4. Ha a talált hibaüzenetek nem nyújtanak elegendő információt a probléma megoldásához, akkor nézze meg az IP szűrő naplót.
5. Az iSeries kommunikációs nyomkövetése szintén olyan hely, ahol szintén találhat általános információkat arról, hogy a helyi rendszer fogadja vagy küldi-e a kapcsolati kéréseket.
6. A TCP alkalmazás nyomkövetése (TRCTCPAPP) parancs egy újabb lehetőség a problémák elkülönítésére. Az IBM szerviz általában a TRCTCPAPP parancsot használja a kapcsolati problémák elemzéséhez használt nyomkövetési kimenet megszerzéséhez.

További ellenőrzendő elemek

Ha egy hiba a kapcsolat beállítása után következik be, és nem biztos benne, hogy hálózati hiba történt-e, akkor próbálkozzon meg a környezet összetettségének csökkentésével. A VPN kapcsolat minden alkotórészének egyidejű vizsgálata helyett kezdje például magával az IP kapcsolattal. Az alábbi lista néhány alapvető irányvonalat ír le a VPN problémák elemzésének megkezdéséhez, kezdve a legegyszerűbb IP kapcsolattal, és fokozatosan haladva az összetettebb VPN kapcsolat felé:

1. Kezdje a helyi és távoli hoszt IP konfigurációjával. Távolítson el minden IP szűrőt a helyi és a távoli rendszeren is a kommunikációhoz használt csatolókról. Tudja pingelni a helyi hosztról a távoli hosztot?

   > **Megjegyzés:** A PING parancs kiadásakor ne feledje el behívni a további paramétereket. Írja be a távoli rendszer címét, nyomja meg a PF10 billentyűt a további paraméterek megadásához, majd írja be a helyi Internet címet. Ez különösen akkor fontos, ha a rendszer több fizikai vagy logikai csatolóval rendelkezik. Ez biztosítja ugyanis, hogy a PING csomagokba a megfelelő címek kerüljenek.

   Ha a válasz **igen**, akkor folytassa a 2. lépéssel. Ha a válasz **nem**, akkor ellenőrizze az IP konfigurációt, a csatoló állapotát és az útvonalkezelési bejegyzéseket. Ha a konfiguráció helyes, akkor egy kommunikációs nyomkövetés segítségével ellenőrizze, hogy a PING kérés elhagyja-e a rendszert. Ha a PING kérés kimegy, de nem érkezik rá válasz, akkor probléma valószínűleg a hálózatban vagy a távoli rendszerben keresendő.

   > **Megjegyzés:** Elképzelhető, hogy az útvonal IP szűrést végző köztes útválasztókon vagy tűzfalakon halad át, amelyek lehet, hogy kiszűrik a PING csomagokat. A PING általában az ICMP protokollon alapul. Ha a PING sikeres, akkor tudható, hogy a csatlakozás adott. Ha a PING sikertelen, akkor csak annyi tudható, hogy a PING meghiúsult. Ilyenkor a kapcsolat ellenőrzéséhez megpróbálkozhat más IP protokollok, például Telnet vagy FTP használatával.
2. Ellenőrizze a VPN szűrőszabályokat, és győződjön meg róla, hogy az aktiválásuk megtörtént. A szűrés sikeresen elindul? Ha **igen**, akkor folytassa a 3. lépéssel. Ha **nem**, akkor nézze meg az iSeries

navigátor Csomagszabályok ablakának hibaüzeneteit. Győződjön meg róla, hogy a szűrőszabályok semmilyen VPN forgalomhoz nem írnak elő hálózati cím fordítást (NAT).

3. Indítsa el a VPN kapcsolatot. A kapcsolat sikeresen elindul? Ha **Igen**, akkor folytassa a 4. lépéssel. Ha **nem**, akkor nézze meg, hogy a a QTOVMAN és QTOKVPNIKE munkanaplók milyen hibákat tartalmaznak.
   VPN használata esetén az Internet szolgáltatónak (ISP), illetve a hálózat valamennyi biztonsági átjárójának támogatnia kell a Hitelesítési fejléc (AH) és a Beágyazott biztonsági kiterjesztés (ESP) protokollt. Az AH vagy ESP használata a VPN kapcsolatnak megadott ajánlásokon múlik.
4. Képes felhasználói szekciót indítani a VPN kapcsolat felett? Ha **igen**, akkor a VPN kapcsolat megfelelően működik. Ha **nem**, akkor ellenőrizze, hogy a csomagszabályok vagy a VPN dinamikus kulcsú csoportok és kapcsolatok tartalmaznak-e olyan szűrőket, amelyek megakadályozzák a felhasználói adatforgalmat.

Általános VPN konfigurációs hibák és kijavításuk

Ez a szakasz írja le a VPN használata során felmerülő általánosabb hibákat, és nyújt tippeket a kijavításukhoz.

Megjegyzés: VPN beállításakor valójában több különböző konfigurációs objektum jön létre, és ezek mindegyike szükséges a VPN kapcsolatok működéséhez. A VPN grafikus felhasználói felületének szóhasználatában ezek az IP biztonsági stratégiák és a Védett kapcsolatok. Vagyis ha a témakör egy objektumra hivatkozik, akkor a VPN ezen objektumainak valamelyikére hivatkozik.

Általános hibaüzenetek

Üzenet	Tünet
TCP5B28	A szűrőszabályok aktiválására tett kísérlet során **TCP5B28: CONNECTION_DEFINITION sorrend megsértés** üzenet érkezik.
Elem nem található	Amikor a jobb egérgombbal egy egy VPN objektumra kattint, és kiválasztja az előugró menü **Tulajdonságok** vagy **Törlés** menüpontját, akkor **Elem nem található** üzenet érkezik.
Érvénytelen PINBUF paraméter	Egy kapcsolat indításának megkísérlésekor **Érvénytelen PINBUF paraméter...** üzenet érkezik.
Elem nem található, távoli kulcsszerver...	Egy dinamikus kulcsú kapcsolat **Tulajdonságok** menüpontjának kiválasztásakor hibaüzenet jelenik meg, mely szerint a szerver nem találja a megadott távoli kulcsszervert.
Nem lehet frissíteni az objektumot	Dinamikus kulcsú vagy kézi kapcsolatok adatlapján az **OK** gomb megnyomásakor megjelenik egy üzenet, mely szerint a szerver nem tudja frissíteni az objektumot.
Nem lehet titkosítani a kulcsokat...	Megjelenik egy üzenet, mely szerint a rendszer nem tudja titkosítani a kulcsokat, mivel a QRETSVRSEC rendszerváltozó értéke nem 1.
CPF9821	Amikor megpróbálja kibontani az iSeries navigátor IP stratégiák mappáját, akkor egy **CPF9821 - Nem jogosult a QSYS könyvtár QTFRPRS programjának használatára** üzenet jelenik meg.

További lehetséges problémák

Hiba	Tünet

Minden kulcs üres	Egy kézi kapcsolat tulajdonságainak megjelenítésekor a kapcsolat minden előzetesen megosztott kulcsa és algoritmus kulcsa üres.
Egy másik rendszer bejelentkezés ablaka jelenik meg	Az iSeries navigátor Csomagszabályok felületének első használatakor az aktuális rendszertől eltérő rendszer bejelentkezés párbeszédablaka jelenik meg.
Nincs kapcsolati állapot	Az iSeries navigátor ablakban az egyik kapcsolat **Állapot** oszlopa üres.
Továbbra is engedélyezett leállt kapcsolatok	Egy kapcsolat leállítása után az iSeries navigátor ablakban a kapcsolat még mindig engedélyezettnek látszik.
3DES titkosítás nem választható	IKE stratégia átalakítás, adat stratégia átalakítás vagy kézi kapcsolat kezelésekor a 3DES titkosítási algoritmus nem jelenik meg.
Váratlan oszlopok megjelenése	Beállította az iSeries navigátorban a VPN kapcsolatoknál megjelenő oszlopokat, viszont amikor később visszatér, más oszlopok jelennek meg.
Aktív szűrőszabályok nem állíthatók le	Amikor megpróbálja leállítani az aktuális szűrőszabály készletet, akkor az eredmények ablakában az Aktív szabályok leállítása meghiúsult üzenet jelenik meg.
Egy kapcsolat dinamikus kulcsú csoportja megváltozik	Egy dinamikus kulcsú kapcsolat létrehozásakor megad egy dinamikus kulcsú csoportot és egy távoli kulcsszerver azonosítót. Később a kapcsolódó konfigurációs objektum megtekintésekor az Általános lapon ugyanaz a kulcsszerver azonosító jelenik meg, de egy másik dinamikus kulcsú csoport társaságában.

VPN hibaüzenet: TCP5B28

Tünet:

Amikor aktiválni próbálja a szűrőszabályokat egy adott csatolón, akkor a következő hibaüzenet érkezik:

TCP5B28: CONNECTION_DEFINITION sorrend megsértés

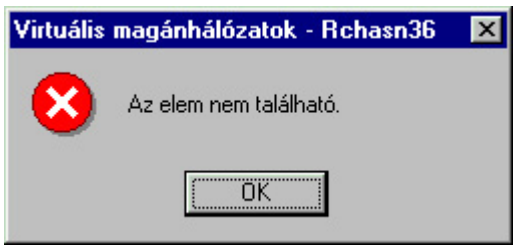
Lehetséges megoldás:

Az aktiválni próbált szűrőszabályok olyan kapcsolatmeghatározásokat tartalmaztak, amelyek egy korábbak aktivált szabálykészletben másként voltak rendezve. A hiba elhárításának legegyszerűbb módja, ha a szabályokat egy adott csatoló helyett **minden csatolón** aktiválja.

VPN hibaüzenet: Elem nem található

Tünet:

Amikor a Virtuális magánhálózatok ablakban a jobb gombbal kattint egy elemre, és kiválasztja az előugró menü **Tulajdonságok** vagy **Törlés** menüpontját, akkor a következő üzenet jelenik meg:



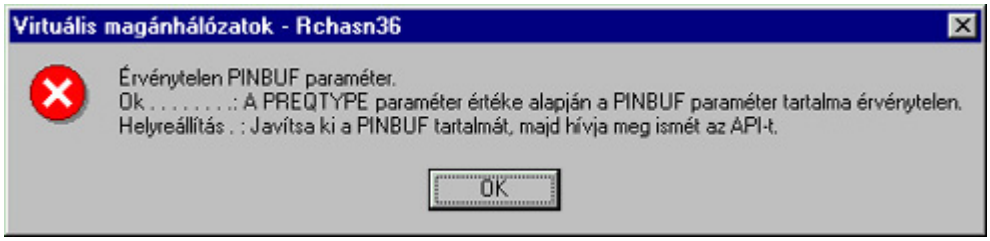
Lehetséges megoldás:

- Elképzelhető, hogy törölte vagy átnevezte az objektumot, de még nem frissítette az ablakot. Ennek következtében az objektum még mindig látható a Virtuális magánhálózatok ablakban. Ennek ellenőrzéséhez válassza a **Nézet** menü **Frissítés** menüpontját. Ha az objektum még mindig megjelenik a Virtuális magánhálózat ablakban, akkor folytassa a hibaelhárítási lista következő bejegyzésénél.
- Az objektum tulajdonságainak beállítása közben elképzelhető, hogy kommunikációs hiba történt a VPN szerver és az iSeries között. A Virtuális magánhálózat ablak több objektuma is a VPN stratégia adatbázis egynél több objektumához kapcsolódik. Ez azt jelenti, hogy egy kommunikációs hiba hatására az adatbázis bizonyos objektumai továbbra is kapcsolódnak egy VPN objektumhoz. Minden egyes alkalommal, amikor egy objektum létrehozását vagy frissítését végzi, egy hibának kell történnie az összehangolás tényleges megszűnésekor. A probléma megoldásának egyetlen módja, ha a hibaüzenet ablak **OK** gombjára kattint. Ez megjeleníti a hibás objektum adatlapját. Az adatlapnak csak a név mezője van kitöltve. Minden más üres (vagy alapértelmezett értékeket tartalmaz). Adja meg az objektum helyes jellemzőit, majd kattintson az **OK** gombra a változások mentéséhez.
- Hasonló hiba történi, ha megpróbálja törölni az objektumot. A probléma kijavításához töltse ki az üzenet **OK** gombjának megnyomásakor megjelenő üres adatlapokat. Ez frissíti a VPN stratégia adatbázis elveszett hivatkozásait. Most már törölhető az objektum.

VPN hibaüzenet: Érvénytelen PINBUF paraméter

Tünet:

Egy kapcsolat indítására tett kísérlet során az alábbihoz hasonló üzenet jelenik meg:



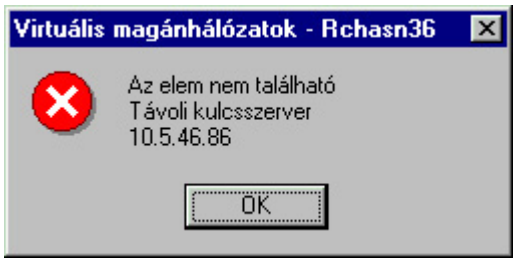
Lehetséges megoldás:

Ez akkor történik, ha a rendszer olyan helyszín használatára van beállítva, amelyben a kisbetűkre való leképezés nem működik megfelelően. A hiba kijavításához győződjön meg róla, hogy minden objektumnak csak nagybetűs neve van, vagy módosítsa a rendszer területi beállításait.

VPN hibaüzenet: Elem nem található, távoli kulcsszerver...

Tünet:

Egy dinamikus kulcsú kapcsolat **Tulajdonságok** menüpontjának kiválasztásakor az alábbihoz hasonló hibaüzenet jelenik meg:



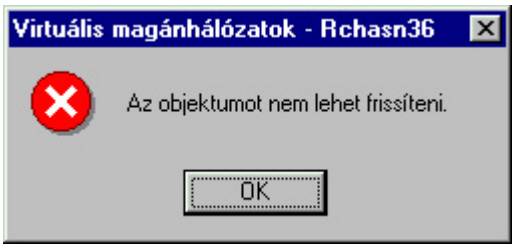
Lehetséges megoldás:

Ez akkor történik, ha egy kapcsolatot egy adott távoli kulcsszerver azonosítóval hoz létre, majd a távoli kulcsszervert eltávolítják a dinamikus kulcsú csoportjából. A hiba kijavításához kattintson a hibaüzenet **OK** gombjára. Ez megnyitja a hibás dinamikus kulcsú kapcsolat adatlapját. Itt egyrészről visszahelyezheti a távoli kulcsszervert a dinamikus kulcsú csoportjába, vagy kiválaszthat egy másik távoli kulcsszerver azonosítót. Kattintson az adatlap **OK** gombjára a változások mentéséhez.

VPN hibaüzenet: Nem lehet frissíteni az objektumot

Tünet:

Dinamikus kulcsú vagy kézi kapcsolatok adatlapján az **OK** gomb megnyomásakor az alábbi üzenet jelenik meg:



Lehetséges megoldás:

Ez a hiba akkor következik be, ha egy aktív kapcsolat által használt objektumot próbál módosítani. Az aktív kapcsolatok objektumai nem módosíthatók. Az objektum módosításához azonosítsa az érintett aktív kapcsolatot, kattintson rá a jobb egérgombbal, majd válassza az előugró menü **Leállítás** menüpontját.

VPN hibaüzenet: Nem lehet titkosítani a kulcsot...

Tünet:

A következő hibaüzenet jelenik meg:

Lehetséges megoldás:

A QRETSVRSEC rendszerváltozó határozza meg, hogy a rendszer tárolhat-e titkosított kulcsokat. Ha az érték 0, akkor a kézi kapcsolatok előzetesen megosztott kulcsai és algoritmus kulcsai nem tárolhatók a VPN stratégia adatbázisban. A probléma kijavításához jelentkezzen be egy 5250 emulációs szekcióval a rendszerre. Írja be a WRKSYSVAL parancsot a parancssorba, majd nyomja meg az **Entert**. Keresse meg a lista QRETSVRSEC bejegyzését, majd írjon be mellé egy 2-est (Módosítás). A következő képernyőn adja meg az 1 értéket, majd nyomja meg az **Entert**.

VPN hibaüzenet: CPF9821

Tünet:

Amikor megpróbálja kibontani az iSeries navigátor IP stratégiák mappáját, akkor egy CPF9821 - Nem jogosult a QSYS könyvtár QTFRPRS programjának használatára üzenet jelenik meg.

Lehetséges megoldás:

Elképzelhető, hogy nem rendelkezik megfelelő jogosultsággal a Csomagszabályok vagy a VPN kapcsolatkezelő jelenlegi állapotának lekérdezéséhez. Győződjön meg róla, hogy rendelkezik *IOSYSCFG jogosultsággal. Ennek megléte esetén hozzá kell tudni férnie az iSeries navigátor csomagszabály funkcióihoz.

VPN hiba: Minden kulcs üres

Tünet:

A kézi kapcsolatok minden előzetesen megosztott kulcsa és algoritmus kulcsa üres.

Lehetséges megoldás:

Ez mindig bekövetkezik, ha a QRETSVRSEC rendszerváltozó értéke 0. A rendszerváltozó nullára állítása

törli a VPN stratégia adatbázis valamennyi kulcsát. A probléma kijavításához a rendszerváltozót 1-re kell állítani, majd ismét meg kell adni minden kulcsot. További információkat a VPN hibaüzenet: Nem lehet titkosítani a kulcsot című témakörben talál.

VPN hiba: Csomagszabályok használatakor egy másik rendszer bejelentkezés ablaka jelenik meg

Tünet:
A Csomagszabályok első használatakor az aktuális rendszertől eltérő rendszer bejelentkezés párbeszédablaka jelenik meg.

Lehetséges megoldás:
A csomagszabályok funkció Unicode formátumban tárolja a biztonsági szabályokat az integrált fájlrendszerben. A kiegészítő bejelentkezés teszi lehetővé az iSeries Access számára a megfelelő Unicode átalakítási tábla megszerzését. Ennek csak egyszer szabad bekövetkeznie.

VPN hiba: Kapcsolati állapot üres az iSeries navigátor ablakban

Tünet:
Az iSeries navigátor ablakban az egyik kapcsolat **Állapot** oszlopa üres.

Lehetséges megoldás:
Az üres állapot azt jelenti, hogy a kapcsolat az indítási folyamat közepén jár. Más szavakkal még nem fut, de még hiba sem érkezett. Az ablak frissítése után a Hiba, Engedélyezett, Kérésre létrehozott vagy Várakozik állapotok valamelyikének kell megjelennie.

VPN hiba: Kapcsolat állapota engedélyezett a leállítás után

Tünet:
Egy kapcsolat leállítása után az iSeries navigátor ablakban a kapcsolat még mindig engedélyezettnek látszik.

Lehetséges megoldás:
Ez általában akkor következik be, ha még nem frissítette az iSeries navigátor ablakát. Vagyis az ablak elavult információkat tartalmaz. A probléma kijavításához válassza a **Nézet** menü **Frissítés** menüpontját.

VPN hiba: 3DES titkosítás nem választható

Tünet:
IKE stratégia átalakítás, adat stratégia átalakítás vagy kézi kapcsolat kezelésekor a 3DES titkosítási algoritmus nem jelenik meg.

Lehetséges megoldás:
A probléma legvalószínűbb oka, hogy a rendszeren csak a Cryptographic Access Provider AC2 (5722-AC2) termék van telepítve, nem pedig a Cryptographic Access Provider AC3 (5722-AC3). Az AC2 a kulcsok hosszával kapcsolatos korlátozások miatt csak a DES titkosítási algoritmus használatát teszi lehetővé.

VPN hiba: Az iSeries navigátor ablakokban váratlan oszlopok jelennek meg

Tünet:
Beállította az iSeries navigátorban a VPN kapcsolatoknál megjelenő oszlopokat, viszont amikor később visszatér, más oszlopok jelennek meg.

Lehetséges megoldás:
A megjelenő oszlopok módosításakor a változások nem felhasználói szintűek, hanem a teljes személyi számítógépre vonatkoznak. Ennek megfelelően ha valaki módosítja az ablakban megjelenő oszlopokat, akkor ez a rendszert használó valamennyi felhasználót érinti.

VPN hiba: Aktív szűrőszabályok nem állíthatók le

Tünet:
Amikor megpróbálja leállítani az aktuális szűrőszabály készletet, akkor az eredmények ablakában az Aktív szabályok leállítása meghiúsult üzenet jelenik meg.

Lehetséges megoldás:
Ez a hiba általában azt jelzi, hogy legalább egy VPN kapcsolat aktív. Le kell állítani minden egyes Engedélyezett állapotú kapcsolatot. Ehhez kattintson a jobb egérgombbal az aktív kapcsolatokon, majd válassza az előugró menü **Leállítás** menüpontját. Most már le kell tudnia állítani a szűrőszabályokat.

VPN hiba: Egy kapcsolat kulcs kapcsolati csoportja megváltozik

Tünet:
Egy dinamikus kulcsú kapcsolat létrehozásakor megad egy dinamikus kulcsú csoportot és egy távoli kulcsszerver azonosítót. Később a kapcsolódó konfigurációs objektum tulajdonságainak megtekintésekor az **Általános** lapon ugyanaz a kulcsszerver azonosító jelenik meg, de egy másik dinamikus kulcsú csoport társaságában.

Lehetséges megoldás:
A dinamikus kulcsú kapcsolat távoli kulcsszerverére vonatkozóan a VPN stratégia adatbázisban tárolt egyedüli információ az azonosító. Amikor a VPN stratégiát keres egy távoli kulcsszerverhez, akkor az első olyan dinamikus kulcsú csoportot nézi meg, amelyben szerepel a távoli kulcsszerver azonosítója. Így az egyik ilyen kapcsolat megjelenítésekor a rendszer a VPN által is megtalált dinamikus kulcsú csoportot használja. Ha a dinamikus kulcsú csoportot nem kívánja társítani a kérdéses távoli kulcsszerverrel, akkor tegye a következők valamelyikét:

1. Távolítsa el a távoli kulcsszervert a dinamikus kulcsú csoportból.
2. A VPN felület bal oldali ablaktábláján bontsa ki a **Csoportonként** mappát, majd a jobb oldali ablaktáblán válassza ki, és húzza át a kívánt dinamikus kulcsú csoportot a táblázat elejére. Ez biztosítja, hogy a VPN ezt a dinamikus kulcsú csoportot ellenőrzi először a távoli kulcsszervernél.

VPN hibaelhárítás a QIPFILTER napló segítségével

A QIPFILTER napló a QUSRSYS könyvtárban található. Ez tartalmazza a szűrőszabály készletekre vonatkozó információkat, illetve az IP adatcsomagok engedélyezésére vagy visszautasítására vonatkozó feljegyzéseket. A naplózás a szűrőszabályokban megadott naplózási beállítás alapján történik.

IP csomagszűrő naplózás engedélyezése
A QIPFILTER napló aktiválásához használja az iSeries navigátor Csomagszabály szerkesztőjét. Minden egyes szűrőszabálynál egyénileg engedélyezni kell a naplózási funkciót. Nincs olyan funkció, amely lehetővé tenni a rendszerre belépő vagy onnan kilépő valamennyi IP adatcsomag naplózását.

Megjegyzés: A QIPFILTER napló engedélyezéséhez a szűrőket le kell állítani.

Egy adott szűrőszabály naplózásának engedélyezéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák** elemeket.
2. Kattintson a jobb egérgombbal a **Csomagszabályok** elemre, majd válassza az előugró menü **Beállítás** menüpontját. Megjelenik a Csomagszabályok felület.
3. Nyisson meg egy meglévő szűrőszabályt.
4. Kattintson duplán a naplózni kívánt szűrőszabályra.
5. Az **Általános** lap **Naplózás** mezőjében válassza a **FULL** beállítást. Ez engedélyezi ennek az adott szűrőszabálynak a naplózását.
6. Kattintson az **OK** gombra.
7. Mentse és aktiválja a megváltozott szűrőszabály fájlt.

Ha egy IP adatcsomag megfelel a szűrőszabály meghatározásainak, akkor a QIPFILTER naplóban létrejön egy bejegyzés.

A QIPFILTER napló használata

Az OS/400 automatikusan létrehozza a naplót az IP csomag szűrés első aktiválása során. A napló bejegyzésre jellemző részleteinek megtekintéséhez jelenítse meg a napló bejegyzéseit a képernyőn, vagy használjon egy kimeneti fájlt.

A naplóbejegyzések kimeneti fájlba másolásával a bejegyzéseket könnyen megtekintheti egy lekérdezési segédprogram, például Query/400 vagy SQL segítségével. Emellett írhat saját HLL programokat is a kimeneti fájlok bejegyzéseinek feldolgozásához.

Egy példa a Napló megjelenítése (DSPJRN) parancsra:

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

A QIPFILTER napló bejegyzéseinek kimeneti fájlba másolásához tegye a következőket:

1. Készítsen másolatot a rendszer által biztosított QSYS/QATOFIPF kimeneti fájlról egy felhasználói könyvtárban az Objektum másodpéldány létrehozása (CRTDUPOBJ) paranccsal. Egy példa a CRTDUPOBJ parancsra:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(könyvtár)
        NEWOBJ(fájl)
   ```

2. A Napló megjelenítése (DSPJRN) paranccsal másolja a QUSRSYS/QIPFILTER napló bejegyzéseit az előző lépésben létrehozott kimeneti fájlba.

Ha a DSPJRN paranccsal nem létező kimeneti fájlba végez másolást, akkor a rendszer létrehozza ugyan a fájlt, ez azonban nem fogja tartalmazni a megfelelő mezőleírásokat.

Megjegyzés: A QIPFILTER napló csak azoknak a szűrőszabályoknak az engedélyezési vagy visszautasítási bejegyzéseit tartalmazza, amelyeknél a naplózási beállítás értéke FULL. Ha például csak PERMIT szűrőszabályokat állít be, akkor a kifejezetten nem engedélyezett IP adatcsomagok visszautasításra kerülnek. Az ilyen visszautasított adatcsomagokról nem készül naplóbejegyzés. Problémaelemzési céllal érdemes létrehozni egy olyan szűrőszabályt, amely kifejezetten visszautasít minden más forgalmat, és emellett FULL naplózásra van állítva. Ezután a naplóban megjelennek a visszautasított IP adatcsomagokra vonatkozó DENY bejegyzések is. Teljesítményszempontok miatt az összes szűrőszabály naplózásának engedélyezése nem javasolt. A szűrőkészletek tesztelésének befejezése után csökkentse a naplózást ésszerű szintre.

A QIPFILTER kimeneti fájl leírását a QIPFILTER napló mezői című témakör táblázata tartalmazza.

QIPFILTER napló mezői

A QIPFILTER kimeneti fájl mezőit a következő táblázat írja le:

Mező neve	Mező hossza	Numerikus	Leírás	Megjegyzések
TFENTL	5	I	Bejegyzés hossza	
TFSEQN	10	I	Sorszám	
TFCODE	1	N	Naplókód	Mindig M
TFENTT	2	N	Bejegyzés típusa	Mindig TF
TFTIME	26	N	SAA időbélyeg	
TFJOB	10	N	Job neve	
TFUSER	10	N	Felhasználói profil	
TFNBR	6	I	Job száma	
TFPGM	10	N	Program neve	
TFRES1	51	N	Fenntartott	
TFUSPF	10	N	Felhasználó	

TFSYMN	8	N	Rendszernév	
TFRES2	20	N	Fenntartott	
TFRESA	50	N	Fenntartott	
TFLINE	10	N	Vonalleírás	*ALL ha a TFREVT értéke U*, Üres, ha a TFREVT értéke L*, illetve a vonal nevét adja meg, ha a TFREVT értéke L.
TFREVT	2	N	Szabály esemény	L* vagy L a szabályok betöltésekor. U* a szabályok leállításakor, és A a szűrő tevékenységek esetén.
TFPDIR	1	N	IP csomag iránya	Az O kimenő, az I bejövő csomagot jelent.
TFRNUM	5	N	Szabály száma	Az aktív szabályfájl szabályszámára vonatkozik.
TFACT	6	N	Végrehajtott szűrő tevékenység	PERMIT, DENY vagy IPSEC
TFPROT	4	N	Szállítási protokoll	1 - ICMP 6 - TCP 17 - UDP 50 - ESP 51 - AH
TFSRCA	15	N	Forrás IP cím	
TFSRCP	5	N	Forrásport	TFPROT = 1 (ICMP) esetén nem tartalmaz használható információkat.
TFDSTA	15	N	Cél IP cím	
TFDSTP	5	N	Célport	TFPROT = 1 (ICMP) esetén nem tartalmaz használható információkat.
TFTEXT	76	N	További szöveg	TFREVT = L* vagy U* esetén leírást tartalmaz.

VPN hibaelhárítás a QVPN napló segítségével

A VPN külön naplót használ az IP forgalomra és kapcsolatokra vonatkozó információk naplózásához. Ez a QVPN napló. A QVPN napló a QSYS könyvtárban található. A naplókód M, a napló típusa TS. A naplóbejegyzésekkel valószínűleg ritkán fog a napi munka részeként találkozni. Hasznosak viszont hibák keresésekor és a rendszer, a kulcsok és a kapcsolatok megfelelő működésének ellenőrzésekor. A naplóbejegyzések segíthetnek annak megértésében, hogy mi történik az adatcsomagokkal. Információkat nyújtanak továbbá a VPN aktuális állapotáról.

VPN napló engedélyezése

A VPN napló aktiválásához használja az iSeries navigátor Virtuális magánhálózatok felületét. Nincs olyan funkció, amely lehetővé tenné minden VPN kapcsolat naplózását. Ennek megfelelően a naplózást külön engedélyezni kell minden egyes dinamikus kulcsú csoport vagy kézi kapcsolat esetében.

Egy adott dinamikus kulcsú csoport vagy kézi kapcsolat naplózási funkciójának engedélyezéséhez tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Hálózat —> IP stratégiák —> Virtuális magánhálózatok —> Védett kapcsolatok** elemeket.
2. Dinamikus kulcsú csoportok esetén bontsa ki a **Csoportonként** bejegyzést, majd kattintson a jobb egérgombbal a dinamikus kulcsú csoportra, amelynek engedélyezni kívánja a naplózását, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kézi kapcsolatok esetén bontsa ki a **Minden kapcsolat** bejegyzést, majd kattintson a jobb egérgombbal a kézi kapcsolatra, amelynek engedélyezni kívánja a naplózását, majd válassza az előugró menü **Tulajdonságok** menüpontját.
4. Az **Általános** lapon válassza ki a kívánt naplózási szintet. Négy lehetőség közül választhat. Ezek a következők:
   Nincs
   A kapcsolati csoportban nem történik naplózás.
   Mind
   Valamennyi kapcsolati tevékenység naplózásra kerül, beleértve a kapcsolat indítását és leállítását, a kulcs frissítését és az IP forgalomra vonatkozó információkat.
   Kapcsolati tevékenység
   A kapcsolati tevékenységek, például a kapcsolat indításának vagy leállításának naplózása.
   IP forgalom
   A kapcsolathoz tartozó valamennyi VPN forgalom naplózásra kerül. Minden szűrőszabály meghívásakor létrejön egy naplóbejegyzés. A rendszer az IP forgalomra vonatkozó információkat a QUSRSYS könyvtár QIPFILTER naplójában naplózza.
5. Kattintson az **OK** gombra.
6. A naplózás aktiválásához indítsa el a kapcsolatot.

Megjegyzés: A naplózás leállítása előtt győződjön meg róla, hogy a kapcsolat inaktív. A kapcsolati csoportok naplózási állapotának módosításakor győződjön meg róla, hogy az adott csoporthoz nem tartoznak aktív kapcsolatok.

A VPN napló használata

A VPN napló bejegyzésre jellemző részleteinek megtekintéséhez jelenítse meg a napló bejegyzéseit a képernyőn, vagy használjon egy kimeneti fájlt.

A naplóbejegyzések kimeneti fájlba másolásával a bejegyzéseket könnyen megtekintheti egy lekérdezési segédprogram, például Query/400 vagy SQL segítségével. Emellett írhat saját HLL programokat is a kimeneti fájlok bejegyzéseinek feldolgozásához. Egy példa a Napló megjelenítése (DSPJRN) parancsra:

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

A VPN napló bejegyzéseinek kimeneti fájlba másolásához tegye a következőket:

1. Készítsen másolatot a rendszer által biztosított QSYS/QATOVSOF kimeneti fájlról egy felhasználói könyvtárban. Ezt a Objektum másodpéldány létrehozása (CRTDUPOBJ) paranccsal teheti meg. Egy példa a CRTDUPOBJ parancsra:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(könyvtár)
        NEWOBJ(fájl)
   ```

2. A Napló megjelenítése (DSPJRN) paranccsal másolja a QUSRSYS/QVPN napló bejegyzéseit az előző lépésben létrehozott kimeneti fájlba. Ha a DSPJRN paranccsal nem létező kimeneti fájlba próbál másolni, akkor a rendszer létrehozza ugyan a fájlt, ez azonban nem fogja tartalmazni a megfelelő mezőleírásokat.

A QVPN kimeneti fájl leírását a QVPN napló mezői című témakör táblázata tartalmazza.

QVPN napló mezői

A QVPN kimeneti fájl mezőit a következő táblázat írja le:

Mező neve	Mező hossza	Numerikus	Leírás	Megjegyzések
TSENTL	5	I	Bejegyzés hossza	
TSSEQN	10	I	Sorszám	
TSCODE	1	N	Naplókód	Mindig M
TSENTT	2	N	Bejegyzés típusa	Mindig TS
TSTIME	26	N	SAA bejegyzés időbélyeg	
TSJOB	10	N	Job neve	
TSUSER	10	N	Job felhasználója	
TSNBR	6	I	Job száma	
TSPGM	10	N	Program neve	
TSRES1	51	N	Nincs használatban	
TSUSPF	10	N	Felhasználói profil neve	
TSSYNM	8	N	Rendszernév	
TSRES2	20	N	Nincs használatban	
TSRESA	50	N	Nincs használatban	
TSESDL	4	I	Jellemző adatok hossza	
TSCMPN	10	N	VPN összetevő	
TSCONM	40	N	Kapcsolat neve	
TSCOTY	10	N	Kapcsolat típusa	
TSCOS	10	N	Kapcsolat állapota	
TSCOSD	8	N	Indítás dátuma	
TSCOST	6	N	Indítás időpontja	
TSCOED	8	N	Befejezés dátuma	
TSCOET	6	N	Befejezés időpontja	
TSTRPR	10	N	Szállítási protokoll	
TSLCAD	43	N	Helyi kliens címe	
TSLCPR	11	N	Helyi portok	
TSRCAD	43	N	Távoli kliens címe	
TSCPR	11	N	Távoli portok	
TSLEP	43	N	Helyi végpont	
TSREP	43	N	Távoli végpont	
TSCORF	6	N	Frissítések száma	

TSRFDA	8	N	Következő frissítés dátuma	
TSRFTI	6	N	Következő frissítés időpontja	
TSRFLS	8	N	Frissítési méretkorlát	
TSSAPH	1	N	SA fázis	
TSAUTH	10	N	Hitelesítés típusa	
TSENCR	10	N	Titkosítás típusa	
TSDHGR	2	N	Diffie-Hellman csoport	
TSERRC	8	N	Hibakód	

VPN hibaelhárítás a VPN munkanaplók segítségével

VPN kapcsolatok problémái esetén mindig érdemes elemezni a munkanaplókat. A VPN környezetről valójában több munkanapló is tartalmaz hibaüzeneteket és további információkat.

Ha a kapcsolat mindkét végpontja iSeries szerver, akkor fontos, hogy a munkanaplók elemzése a kapcsolat mindkét oldalán megtörténjen. A dinamikus kapcsolatok indítási hibáinak esetén például hasznos látni, hogy mi történik a távoli rendszeren.

A QTOVMAN és QTOKVPNIKE jobok a QSYSWRK alrendszerben futnak. A megfelelő munkanaplóikat az iSeries navigátorból tekintheti meg.

Ez a szakasz mutatja be a VPN környezetek legfontosabb jobjait. A következő listában a jobok neve, illetve a jobok felhasználásának rövid leírása látható:

QTCPIP
Ez a job az összes TCP/IP csatoló indítását végző alapvető job. Ha a TCP/IP alapjait érintő általános problémája van, akkor elemezze a QTCPIP munkanaplót.

QTOKVPNIKE
A QTOKVPNIKE a VPN kulcskezelő job. A VPN kulcskezelő az 500-as UDP porton figyel, és az Internet kulcscsere (IKE) protokollal kapcsolatos feldolgozást végzi.

QTOVMAN
Ez a job a VPN kapcsolatok kapcsolatkezelője. A hozzá kapcsolódó munkanapló az összes meghiúsult kapcsolati kísérlet üzeneteit tartalmazza.

QTPPANSxxx
Ez a job a PPP telefonos kapcsolatoknál kerül felhasználásra. Ez a job válaszol az olyan kapcsolati kísérletekre, amelyeknél a PPP profilban *ANS van meghatározva.

QTPPPCTL
Ez a kifelé irányuló telefonos kapcsolat PPP jobja.

QTPPPL2TP
Ez a job kezeli az L2TP protokollt. Ha problémái vannak egy L2TP alagút beállításával, akkor nézze meg ennek a munkanaplónak az üzeneteit.

VPN kapcsolatkezelő általános hibaüzenetei

Ez a szakasz ír le néhányat a VPN kapcsolatkezelő gyakoribb hibaüzenetei közül.

A VPN kapcsolatkezelő a VPN kapcsolatokban felmerült hibák bekövetkezésekor általában két üzenetet naplóz a QTOVMAN munkanaplóba. Az első üzenetben találhatók a hibára vonatkozó részletek. A hibákra

vonatkozó információk megtekintéséhez az iSeries navigátorban kattintson a jobb egérgombbal a hibás kapcsolatra, majd válassza az előugró menü **Hibainformációk** menüpontját.

A második üzenet írja le, hogy milyen művelet végrehajtására tett kísérlet során történt a kapcsolat hibája. Ez például a kapcsolat indítása vagy leállítása lehet. Az alábbiakban leírt TCP8601, TCP8602 és TCP860A üzenetek az ilyen második üzenetek tipikus példái.

VPN kapcsolatkezelő hibaüzenetek

Üzenet	Ok	Helyreállítás
TCP8601 A [*kapcsolat neve*] VPN kapcsolat nem indítható el	A VPN kapcsolat az alábbi ok kódok valamelyike miatt nem indítható el: *0* - A munkanaplónak ugyanerre a VPN kapcsolatnévre vonatkozó egyik korábbi üzenete biztosít részletes információkat. *1* - VPN stratégia beállítás. *2* - Kommunikációs hálózati hiba *3* - A VPN kulcskezelő nem tudott új biztonsági megegyezést egyeztetni. *4* - A kapcsolat távoli végpontja nincs megfelelően beállítva. *5* - A VPN kulcskezelő nem tudott válaszolni a VPN kapcsolatkezelőnek. *6* - A VPN kapcsolat IP biztonsági összetevőjét nem lehet betölteni. *7* - PPP összetevő hiba.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel. 3. Az iSeries navigátorban tekintse meg a kapcsolat állapotát. A nem induló kapcsolatok hibás állapottal jelennek meg.
TCP8602 Hiba történt a [*kapcsolat neve*] VPN kapcsolat leállításakor	A rendszer kezdeményezte a megadott VPN kapcsolat leállítását, de az nem állt le vagy hibásan állt le az alábbi ok kódok valamelyike miatt: *0* - A munkanaplónak ugyanerre a VPN kapcsolatnévre vonatkozó egyik korábbi üzenete biztosít részletes információkat. *1* - A VPN kapcsolat nem létezik. *2* - Belső kommunikációs hiba a VPN kulcskezelővel. *3* - Belső kommunikációs hiba az IPSec összetevővel. *4* - Kommunikációs hiba a VPN kapcsolati végponttal.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel. 3. Az iSeries navigátorban tekintse meg a kapcsolat állapotát. A nem induló kapcsolatok hibás állapottal jelennek meg.

TCP8604 A [*kapcsolat neve*] VPN kapcsolat indítása meghiúsult	A VPN kapcsolat indítása az alábbi ok kódok valamelyike miatt meghiúsult: *1* - A távoli hoszt neve nem fordítható le IP címre. *2* - A helyi hosztnév nem fordítható le IP címre. *3* - A VPN kapcsolathoz társított VPN stratégia szűrőszabály nincs betöltve. *4* - Egy felhasználó által megadott kulcs érték érvénytelen a társított algoritmushoz. *5* - A VPN kapcsolat kezdeményezési értéke nem teszi lehetővé a megadott tevékenységet. *6* - A VPN kapcsolatban az egyik rendszer szerepe nincs összhangban a kapcsolati csoport információival. *7* - Fenntartott. *8* - A VPN kapcsolat adatvégpontjai (helyi és távoli címek és szolgáltatások) nincsenek összhangban a kapcsolati csoport információival. *9* - Érvénytelen azonosítótípus.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel. 3. Az iSeries navigátorban ellenőrizze vagy javítsa ki a VPN stratégia beállításait. Győződjön meg róla, hogy a kapcsolathoz társított dinamikus kulcsú csoportnak elfogadható értékek vannak beállítva.
TCP8605 A VPN kapcsolatkezelő nem tud kommunikálni a VPN kulcskezelővel	A VPN kapcsolatkezelőnek szüksége van a VPN kulcskezelő szolgáltatásaira a dinamikus VPN kapcsolatok biztonsági megegyezéseinek kialakításához. A VPN kapcsolatkezelő nem tud kommunikálni a VPN kulcskezelővel.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. A NETSTAT OPTION(*IFC) paranccsal ellenőrizze, hogy a *LOOPBACK csatoló aktív-e. 3. Az ENDTCPSVR SERVER(*VPN) parancs kiadásával fejezze be a VPN szervert. Ezután indítsa újra a VPN szervert az STRTCPSRV SERVER(*VPN) paranccsal. **Megjegyzés:** Ez valamennyi aktív VPN kapcsolat befejezését vonja maga után.

TCP8606 A VPN kulcskezelő nem tudta kialakítani a kért biztonsági megegyezést a [*kapcsolat neve*] számára	A VPN kulcskezelő nem tudta kialakítani a kért biztonsági megegyezést az alábbi ok kódok valamelyike miatt: *24* - A VPN kulcskezelő kulcs kapcsolati hitelesítése meghiúsult. *8300* - Hiba történt a VPN kulcskezelő kulcs kapcsolat egyeztetésekor. *8306* - Nem található helyi előzetesen megosztott kulcs. *8307* - Nincs távoli stratégia az IKE 1. fázisához. *8308* - Nem található távoli előzetesen megosztott kulcs. *8327* - A VPN kulcskezelő kulcs kapcsolati egyeztetései túllépték az időkorlátot. *8400* - Hiba történt a VPN kulcskezelő VPN kapcsolat egyeztetésekor. *8407* - Nincs távoli stratégia az IKE 2. fázisához. *8408* - A VPN kulcskezelő VPN kapcsolati egyeztetései túllépték az időkorlátot. *8500 vagy 8509* - A VPN kulcskezelő hálózati hibába ütközött.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel. 3. Az iSeries navigátorban ellenőrizze vagy javítsa ki a VPN stratégia beállításait. Győződjön meg róla, hogy a kapcsolathoz társított dinamikus kulcsú csoportnak elfogadható értékek vannak beállítva.
TCP8608 A [*kapcsolat neve*] VPN kapcsolat nem tudott NAT címet szerezni	A dinamikus kulcsú csoport vagy adatkapcsolat hálózati cím fordítást ír elő legalább egy címen, de ez az alábbi ok kódok valamelyike miatt meghiúsult: *1* - A NAT alkalmazási címe nem egyedülálló IP cím. *2* - Minden rendelkezésre álló cím használatban van.	1. Ellenőrizze a munkanaplókban az esetleges további üzeneteket. 2. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel. 3. Az iSeries navigátorban ellenőrizze vagy javítsa ki a VPN stratégiát. Győződjön meg róla, hogy a kapcsolathoz társított dinamikus kulcsú csoport címeinek elfogadható értékek vannak beállítva.
TCP8620 A helyi kapcsolati végpont nem érhető el	A VPN kapcsolat nem engedélyezhető, mivel a helyi kapcsolati végpont nem érhető el.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. A NETSTAT OPTION(*IFC) paranccsal ellenőrizze, hogy a helyi kapcsolati végpont elindult-e. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8621 A helyi adatvégpont nem érhető el	A VPN kapcsolat nem engedélyezhető, mivel a helyi adatvégpont nem érhető el.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. A NETSTAT OPTION(*IFC) paranccsal ellenőrizze, hogy a helyi kapcsolati végpont elindult-e. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.

TCP8622 A szállítási beágyazás nem megengedett átjáró esetén	A VPN kapcsolat nem engedélyezhető, mivel az egyeztetett stratégia szállítás beágyazási módot ír elő, a kapcsolat azonban biztonsági átjáróként van megadva.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban módosítsa a VPN kapcsolathoz társított VPN stratégiát. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8623 A VPN kapcsolat átfedésben van egy meglévővel	A VPN kapcsolat nem engedélyezhető, mivel egy meglévő VPN kapcsolat már engedélyezett. A kapcsolat helyi adatvégpontja [*helyi adatvégpont értéke*], a távoli adatvégpont [*távoli adatvégpont értéke*].	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban jelenítse meg az összes olyan engedélyezett kapcsolatot, amely a kérdéses kapcsolattal megegyező helyi vagy távoli adatvégpontot használ. Ha mindkét kapcsolat szükséges, akkor módosítsa a meglévő kapcsolat stratégiáját. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8624 A VPN kapcsolat nincs a társított stratégia szűrőszabály hatókörében	A VPN kapcsolat nem engedélyezhető, mivel az adatvégpontok nem esnek a megadott stratégia szűrőszabály hatálya alá.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban jelenítse meg a kapcsolat vagy dinamikus kulcsú csoport adatvégpont korlátozásait. Ha a **Stratégia szűrő részhalmaza** vagy a **Stratégia szűrőnek megfelelés testreszabása** beállítás ki van választva, akkor ellenőrizze a kapcsolat adatvégpontjait. Ezeknek az IPSEC tevékenységet és a kapcsolathoz tartozó VPN kapcsolat nevét meghatározó aktív szűrőszabály hatálya alá kell esniük. Módosítsa a meglévő kapcsolat stratégiáját vagy szűrőszabályait a kapcsolat engedélyezéséhez. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8625 A VPN kapcsolat nem tudott teljesíteni egy ESP algoritmus ellenőrzést	A VPN kapcsolat nem engedélyezhető, mivel kapcsolathoz társított titkos kulcs nem elegendő.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban jelenítse meg a kapcsolathoz társított stratégiát, és adjon meg egy másik titkos kulcsot. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.

TCP8626 A VPN kapcsolati végpont nem egyezik meg az adatvégponttal	A VPN kapcsolat nem engedélyezhető, mivel a stratégia szerint ez egy hoszt, de a VPN kapcsolat végpontja nem egyezik meg az adatvégponttal.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban jelenítse meg a kapcsolat vagy dinamikus kulcsú csoport adatvégpont korlátozásait. Ha a **Stratégia szűrő részhalmaza** vagy a **Stratégia szűrőnek megfelelés testreszabása** beállítás ki van választva, akkor ellenőrizze a kapcsolat adatvégpontjait. Ezeknek az IPSEC tevékenységet és a kapcsolathoz tartozó VPN kapcsolat nevét meghatározó aktív szűrőszabály hatálya alá kell esniük. Módosítsa a meglévő kapcsolat stratégiáját vagy szűrőszabályait a kapcsolat engedélyezéséhez. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8628 A stratégia szűrőszabály nincs betöltve	A kapcsolat stratégia szűrőszabálya nem aktív.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban jelenítse meg az aktív stratégia szűrőket. Ellenőrizze a kapcsolat stratégia szűrőszabályait. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP8629 Eldobott VPN kapcsolati IP csomag	A VPN kapcsolat VPN NAT használatát írja elő, de a szükséges NAT címkészlet túllépte a rendelkezésre álló NAT címeket.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Az iSeries navigátorban növelje a VPN kapcsolathoz hozzárendelt NAT címek számát. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.
TCP862A A PPP kapcsolatot nem lehet elindítani	A VPN kapcsolat egy PPP profilhoz tartozik. Indításakor kísérlet történt a PPP profil indítására, de ez hibához vezetett.	1. Ellenőrizze a munkanaplókban a kapcsolatra vonatkozó esetleges további üzeneteket. 2. Ellenőrizze a PPP kapcsolathoz tartozó munkanaplót. 3. Javítsa ki a hibákat, majd próbálkozzon újra a kéréssel.

VPN hibaelhárítás az OS/400 kommunikációs nyomkövetés segítségével

Az iSeries lehetővé teszi a kommunikációs vonalak, például helyi hálózati (LAN) és nagy kiterjedésű hálózati (WAN) csatolók adatainak nyomkövetését. Az átlagos felhasználónak a nyomkövetés adatai valószínűleg nem sokat mondanak. A nyomkövetés bejegyzéseinek segítségével azonban meghatározhatja, hogy a helyi és a távoli rendszer között sor került-e adatcserére.

Kommunikációs nyomkövetés indítása
A rendszer kommunikációs nyomkövetésének indításához használja a Kommunikációs nyomkövetés indítása (STRCMNTRC) parancsot. Egy példa az STRCMNTRC parancsra:

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

A parancs paramétereit a következő lista írja le:

CFGOBJ (Konfigurációs objektum)
A nyomkövetésbe bevonni kívánt konfigurációs objektum neve. Az objektum egy vonalleírás, egy hálózati csatoló leírás vagy egy hálózati szerver leírás lehet.

CFGTYPE (Konfiguráció típusa)
Megadja, hogy vonal (*LIN), hálózati csatoló (*NWI) vagy hálózati szerver (*NWS) nyomkövetése történik.

MAXSTG (Pufferméret)
A nyomkövetés puffermérete. Az alapértelmezett érték 128 KB. A megadható tartomány 128 KB és 64 MB között van. A tényleges maximális rendszerszintű pufferméret a Rendszer szervizeszközökben (SST) adható meg. Ennek megfelelően hibaüzenet érkezhet, ha az STRCMNTRC parancsnak a Rendszer szervizeszközökben beállítottnál nagyobb pufferméretet ad meg. Ne feledje, hogy az összes futó kommunikációs nyomkövetés összesített puffermérete sem haladhatja meg a Rendszer szervizeszközökben megadott maximális pufferméretet.

DTADIR (Adatok iránya)
A nyomon követni kívánt adatforgalom iránya. Az irány lehet csak kimenő forgalom (*SND), csak bejövő forgalom (*RCV) vagy mindkét irányú (*BOTH).

TRCFULL (Nyomkövetés megtelése)
Ez a paraméter határozza meg, mi történik, ha megtelik a nyomkövetési puffer. A paraméternek két lehetséges értéke van. Az alapértelmezett érték a *WRAP, amely azt jelenti, hogy a nyomkövetési puffer megtelésekor a nyomkövetés újrakezdődik. A legújabb nyomkövetési rekordok felülírják a legrégebbi bejegyzéseket.

A *STOPTRC érték lehetővé teszi a nyomkövetés leállását, ha a MAXSTG paraméterben megadott méretű nyomkövetési puffert megtelt nyomkövetési rekordokkal. Általános szabályként a pufferméretet mindig állítsa elég nagyra ahhoz, hogy minden nyomkövetési rekord beleférjen. A nyomkövetés újrakezdésekor fontos nyomkövetési információk veszhetnek el. Ritkán bekövetkező problémák esetén állítsa a nyomkövetési puffert elér nagyra ahhoz, hogy a puffer esetleges újrakezdése ne írjon felül fontos információkat.

USRDTA (Nyomkövetésben szereplő felhasználói byte-ok száma)
Megadja, hogy az adatkeretekből hány byte-nyi felhasználói adat szerepeljen a nyomkövetésben. LAN csatolók esetén alapértelmezésben csak az első 100 byte-nyi felhasználói adat lementésére kerül sor. Minden más csatolónál az összes felhasználói adat mentésre kerül. Ha a keretek felhasználói adataiban gyanítja a hiba okát, akkor adja meg a *MAX értéket.

TEXT (Nyomkövetés leírása)
Megadja a nyomkövetés leírását.

Kommunikációs nyomkövetés leállítása
Ellentétes értelmű beállítás hiányában a nyomkövetés általában leáll a nyomkövetés célját jelentő feltétel bekövetkezésekor. A nyomkövetés egyébként a Kommunikációs nyomkövetés leállítása (ENDCMNTRC) paranccsal állítható le. Egy példa az ENDCMNTRC parancsra:

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

A parancs két paraméterrel rendelkezik:

CFGOBJ (Konfigurációs objektum)
A konfigurációs objektum neve, amelyen jelenleg fut a nyomkövetés. Az objektum egy vonalleírás, egy hálózati csatoló leírás vagy egy hálózati szerver leírás lehet.

CFGTYPE (Konfiguráció típusa)
Megadja, hogy vonal (*LIN), hálózati csatoló (*NWI) vagy hálózati szerver (*NWS) nyomkövetése történik.

Nyomkövetési adatok nyomtatása
A kommunikációs nyomkövetés leállítása után a nyomkövetési adatokat ki kell nyomtatni. Ehhez használja a Kommunikációs nyomkövetés nyomtatása (PRTCMNTRC) parancsot. Mivel a nyomkövetési időszak során a vonal teljes forgalma lementésre kerül, a kimenet előállítás során alkalmazott szűrésre több lehetőség is rendelkezésre áll. A spoolfájl méretét ajánlott a lehető legkisebben tartani. Ez gyorsabbá és hatékonyabbá teszi az elemzést. VPN problémák esetén csak az IP forgalmat kell figyelni, és lehetőség szerint azt is csak egy adott IP címre vonatkozóan. Lehetőség van IP portszám alapján végzett szűrésre is. Egy példa a PRTCMNTRC parancsra:

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

Ebben a példában a nyomkövetés IP forgalomnak megfelelően kerül formázásra, és csak azokat az adatokat tartalmazza, ahol a forrás- vagy célcím 10.50.21.1, és a forrás- vagy célport 500.

Az alábbiakban csak a VPN problémák elemzése szempontjából legfontosabb paramétereket írjuk le:

CFGOBJ (Konfigurációs objektum)
A konfigurációs objektum neve, amelyen jelenleg fut a nyomkövetés. Az objektum egy vonalleírás, egy hálózati csatoló leírás vagy egy hálózati szerver leírás lehet.

CFGTYPE (Konfiguráció típusa)
Megadja, hogy vonal (*LIN), hálózati csatoló (*NWI) vagy hálózati szerver (*NWS) nyomkövetése történik.

FMTTCP (TCP/IP adatok formázása)
Megadja, hogy a formázás TCP/IP vagy UDP/IP adatoknak megfelelően történik-e. IP adatoknak megfelelő formázáshoz adja meg a *YES értéket.

TCPIPADR (TCP/IP adatok formázása cím alapján)
A paraméter két elemből áll. Ha mindkét elemben IP címeket ad meg, akkor csak az adott címek közötti IP forgalom kerül nyomtatásra.

SLTPORT (IP portszám)
A szűrni kívánt IP portszám.

FMTBCD (Üzenetszórás adatok formázása)
Megadja, hogy nyomtatásra kerüljenek-e az üzenetszórásos adatok. Az alapértelmezett beállítás a *YES. Ha nem kívánja befoglalni mondjuk a Címfeloldási protokoll (ARP) kéréseket, akkor adja meg a *NO értéket, ellenkező esetben a kimenetet teljesen ellephetik az üzenetszórásos csomagok.

VPN kapcsolódó információk

További VPN példahelyzeteket a virtuális magánhálózatokkal kapcsolatos alábbi információforrásokban találhat:

- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM iSeries Server with Windows 2000 VPN Clients, REDP0153** 

Ez az IBM kiadvány lépésenként megadott útmutatásokat tartalmaz a V5R1 kiadású iSeries szerverek és Windows 2000 kliensek közötti VPN alagutak kialakításához a Windows 2000 saját L2TP és IPSec támogatásának felhasználásával.

- **AS/400 Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00** 
  Ez a kiadvány a VPN alapelveket mutatja be, emellett leírja ezek megvalósítását az IPSec és L2TP protokoll felhasználásával az OS/400 rendszereken.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00** 
  Ez a kiadvány az AS/400 rendszerek valamennyi hálózati biztonsági szolgáltatását bemutatja, köztük az IP szűrést, a hálózati cím fordítást, a virtuális magánhálózatokat, a HTTP proxy szervereket, az SSL protokollt, valamint a DNS, levéltovábbítási, megfigyelési és naplózási szolgáltatásokat. Az egyes szolgáltatások használatára gyakorlati példákat is bemutat.

- **Virtual Private Networking: Securing Connections** 
  Ez a weboldal emeli ki a fontosabb VPN híreket, sorolja fel a legfrissebb javításokat, és további érdeklődésre számot tartó webhelyek hivatkozásait tartalmazza.
- **Biztonsággal kapcsolatos további kézikönyvek és kiadványok**
  Itt találja a biztonsággal kapcsolatos online kiadványok listáját.

A PDF fájl mentése a munkaállomáson megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF hivatkozásra a böngészőben (a fenti hivatkozás).
2. Válassza az előugró menü **Cél mentése másként...** menüpontját.
3. Válassza ki a könyvtárat, amelybe a PDF fájlt menteni kívánja.
4. Kattintson a **Mentés** gombra.

A PDF fájlok megtekintéséhez és nyomtatásához szükség van az Adobe Acrobat Reader programra, amely letölthető az Adobe webhelyéről (www.adobe.com/prodindex/acrobat/readstep.html). 

Nyomtatva Dániában