

A hálózati költségek csökkentése virtuális magánhálózatokkal

• Kész a 2000. évre

Novell®

BorderManager™

VIRTUÁLIS MAGÁNHÁLÓZATOK

TARTALOMJEGYZÉK

FEJEZET 1

Vezetői összefoglaló	1
----------------------	---

FEJEZET 2

A VPN-ek követelményei	2
------------------------	---

FEJEZET 3

Egy VPN felépítése	3
A hálózati réteg biztosítása	3
A biztonsági kulcsok felügyelete	4

FEJEZET 4

BorderManager VPN Services 3	5
Telephelyek közötti VPN	5
Kliens és szerver közötti VPN	6

FEJEZET 5

Architektúra	7
Szabványalapúság	7
NDS-integráció	7

FEJEZET 6

Telephelyek közötti VPN kialakítása BorderManager VPN Services 3-mal	8
Telepítés és beállítások	8
Alagutak automatikus létrehozása	9
Dinamikus útválasztás	9

FEJEZET 7

Kliens és telephely közötti VPN kialakítása BorderManager VPN Services 3-mal	10
Automatikus konfiguráció és alagutak kialakítása	11
A kapcsolat aktivitásának figyelése	13

FEJEZET 8

A BorderManager Enterprise Edition 3 internetes biztonsági felügyeleti csomag része	13
NDS-integráció	14

FEJEZET 9

Összefoglalás	14
---------------	----

CÍMTÁRALAPÚ VPN-MEGOLDÁS A BIZTONSÁG, A TELJESÍTMÉNY ÉS A FELÜGYELHETŐSÉG FELÁLDOZÁSA NÉLKÜL

A virtuális magánhálózatok (VPN-ek) gazdaságos, ugyanakkor biztonságos módot kínálnak a távoli telephelyek összekapcsolására, illetve a távoli felhasználók hálózati hozzáféréseinek biztosítására. VPN-ek kialakításakor azonban számításba kell venni néhány fontos tényezőt. A jelen ismertető bemutatja a VPN-eket, valamint egy valóban hatékony megoldás kialakításához szükséges feltételeket. Részletesen ismerteti továbbá a Novell BorderManager VPN Services 3-at – egy átfogó megoldást, amely mindezen feltételeknek megfelel.

VEZETŐI ÖSSZEFOGLALÓ

Hosszú éveken keresztül az volt a szokás, hogy a vállalatok saját nagytávolságú hálózati kapcsolatokat üzemeltettek, és ezeken keresztül kapcsolódtak a távoli telephelyekhez, esetleg üzleti partnereikhez, például a beszállítókhöz és nagykereskedőkhöz. Ezek a nagytávolságú hálózatok jellemzően bérelt telefonvonalak voltak. Emellett sok cégnél szokás volt modemfarmokat telepíteni, amelyeken keresztül a felhasználók távolról, behívásos telefonkapcsolaton keresztül csatlakozhattak a vállalati hálózatokra.

E hagyományos megoldásnak megvannak a maga hátulütői – a legnagyobb mindjárt a költség. A bérelt vonalak drágák, a modembankok vásárlása és fenntartása nemkülönb. Ráadásul a behíváshoz szükséges távolsági telefonkapcsolatok igen költségessé teszik a messziről történő hozzáférést a hálózathoz. A távoli behívásos kapcsolatok másik örökletes baja a nem megfelelő biztonság, hiszen az adatok a nyilvános telefonhálózaton keresztül továbbítódnak.

Vonzó megoldást nyújtanak mindezen problémákra a virtuális magánhálózatok (VPN-ek). A VPN-ek az Internet infrastruktúráját használják fel a telephelyek összekötésére, illetve a távoli behívásos kapcsolatok kialakítására. Az Internet közel univerzális kiterjedése révén nincs többé szükség saját bérelt vonalakra és modemfarmokra; hasonlóképpen, megszűnnek a távolsági telefonhívások is. Mindennek eredményeképpen a VPN-ek sokkal olcsóbbak, mint a hagyományos nagytávolságú kapcsolatok: a legtöbb cég 20–70 százalék közötti megtakarítást ér el VPN-ek használatával.

VPN-ek kialakíthatók a vállalati intraneteken is. Saját hálózatok hozhatók létre az intraneten belül, mondjuk egy adott osztály vagy egy bizalmas adatokkal dolgozó csoport számára. Megoldható például, hogy földrajzilag különálló helyszínen dolgozó mérnökök együttműködjenek egy új, titkos projekten, és megoszthassák egymással az adatokat anélkül, hogy félteniük kellene azokat a jogosulatlan hozzáféréstől.

Az alábbi dokumentumban összegyűjtöttük a legfontosabb tényezőket, amelyeket figyelembe kell vennünk egy VPN kialakításakor, és azokat a követelményeket, amelyeknek egy valóban hatékony megoldást nyújtó VPN-nek meg kell felelnie. Ismertetjük, hogyan működnek a VPN-ek, áttekintjük a hálózati szabványokat, amelyekre működésük alapul. Végezetül bemutatjuk a Novell VPN-megoldását – a BorderManager VPN Services 3-at, a BorderManager Enterprise Edition 3, a Novell internetes biztonsági felügyeleti csomagjának részét.

A VPN-EK KÖVETELMÉNYEI

VPN-ek kialakításakor két fontos tényezőt kell mindenképpen figyelembe vennünk. Az első ezek közül a biztonság. A bérelt magánvonalak biztonságosak, ám az Internet, lévén nyílt hálózat, híresen nem az. Éppen ezért minden szervezetnek különös gondot kell fordítania arra, hogy a VPN védve legyen a jogosulatlan hozzáférések ellen. Ebbe beletartozik az internetes buherátorok távoltartása, a VPN-adatok titkosítása a lehallgatás ellen, valamint az adatforgalom szándékos rongálásának megakadályozása. A második a sávszélesség. Az Interneten keresztül jellemzően sokkal alacsonyabb sávszélesség érhető el, mint bérelt vonalakkal. Éppen ezért ügyelni kell arra, hogy a VPN teljesítménye elegendő legyen, ne rontsa le a felhasználók termelékenységét.

Ahhoz, hogy valóban hatékonyan működjön, számos feltételnek kell megfelelnie egy VPN-nek:

- **Megbízhatóság.** A VPN-nek biztosítania kell a rajta áthaladó adatok védelmét lehallgatás ellen.

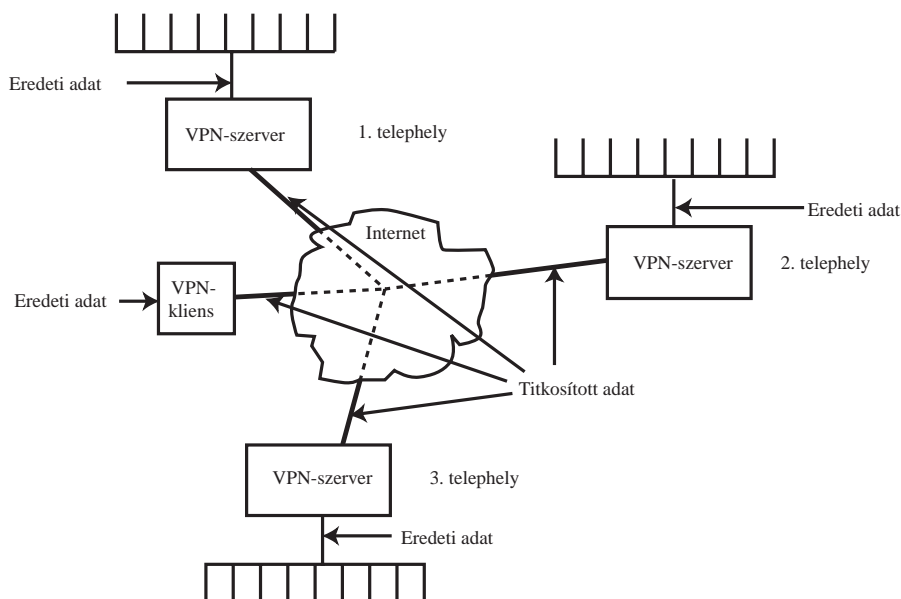
- **Hitelesség.** A VPN-nek biztosítania kell, hogy a rajta dolgozó emberek valóban egy meghatározott közösség tagjai. Emellett a VPN-nek biztosítania kell az adatok és az adatforrások hitelességét, vagyis azt, hogy a küldő valóban az, akinek mondja magát.

- **Integritás.** A VPN-nek biztosítania kell, hogy a megérkezett adatok valóban pontosan megegyezzenek az elküldött adatokkal, vagyis védenie kell az adatokat az átviteli hibáktól és a szándékos rongálástól.

- **Többféle protokoll kezelése.** Bár az Internet tiszta IP alapú, NetWare-felhasználók milliói használják a mai napig IPX-et. Éppen ezért célszerű, ha a VPN képes nemcsak az IP-t, hanem az IPX-et is kezelni.

- **Képes mind telephelyek közötti, mind kliensek és telephelyek közötti kapcsolatra.** A VPN-nek képesnek kell lennie nemcsak az egyes telephelyek összekapcsolására, hanem a távolról behívó felhasználók kiszolgálására is.

1. ábra. VPN-alagutak



- *Kezelnie kell a meglévő és jövőbeni VPN-szabványokat. A VPN-nek feltétlenül szabványalapúnak kell lennie, hiszen csak így biztosítható a különféle gyártók eszközei közötti kölcsönös együttműködés és az, hogy a cégek maguk választhassák ki az igényeiknek legjobban megfelelő megoldást. A szabványalapúság ezenfelül nyitva hagyja a lehetőségeket a mindig legmodernebb technológiák használata előtt.*
- *Optimalizált teljesítmény. A VPN legyen képes maximálisan kihasználni az Internet korlátozott sávszélességét.*

EGY VPN FELÉPÍTÉSE

A VPN-ek az adatokat ún. „alagutakon” (tunnel) keresztül továbbítják az Interneten vagy a vállalati intraneten. Az alagutak az Internetet vagy a vállalati intranetet kapcsolati médiumként használó biztonságos, titkosított virtuális kapcsolatok. Telephelyek közötti VPN esetében szerverek közötti alagutak, kliens–telephely VPN esetében kliensek és szerverek közötti alagutak jönnek létre. (Ld. az előző oldal 1. ábráját.)

A VPN minden egyes IP- (vagy IPX-) csomagot titkosít és beágyaz, mielőtt továbbítaná az alagúton keresztül. A beágyazott csomag tartalmaz a hitelesítéshez, az adat és a forrás azonosításához szükséges adatokat. Ezen hitelesítési adatok alapján ellenőrzi a VPN az adatok integritását is, azt, hogy az eredeti adat nem sérült meg a továbbítás során.

A HÁLÓZATI RÉTEG BIZTOSÍTÁSA

A VPN alagútmechanizmust az IPSec (IP Security) nevű szabvány (RFC # 1825-1827) definiálja. Az eredeti IP- (vagy IPX-) csomagok titkosítva, VPN-alagútcsomagokba beágyazva továbbítódnak az Interneten. A 2. ábra bemutatja a VPN-alagútcsomag formátumát, amennyiben az IPSec és a SKIP (Simple Key exchange Internet Protocol) szabványokat együtt használjuk. A SKIP-et alább részletesen ismertetjük.

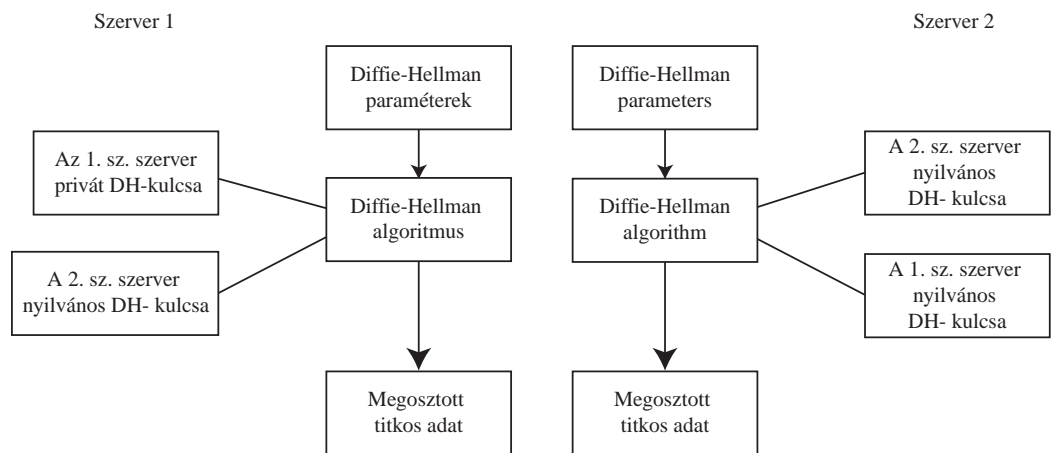
A csomag egyes részei:

- *Forráscím. A VPN-forrásszervert vagy -klienst azonosítja. Az eredeti küldő személyazonossága titokban marad, ezzel is növelve a biztonságot.*
- *Célcím. A VPN-célszervert vagy -klienst azonosítja. A fogadó személyazonossága titokban marad, ezzel is növelve a biztonságot.*
- *(A SKIP IETF ajánlása alapján definiált) kulcsfelügyeleti (SKIP) fejléc. A csomagban használt kulcsot, algoritmust és a következő protokollt határozza meg.*
- *Hitelesítési fejléc (Authentication Header, AH, az RFC 1826-nak megfelelően). Az adatok és a forrás hitelességét biztosító hitelesítési adatokat tartalmazza. A VPN a hitelesítési fejléct az alábbi négy szabványos átalakítás valamelyikével végzi: 128 bites kulcsolt MD5 (az RFC 1828-ban definiált módon), 128 bites HMAC-MD5-tel (az RFC 2104-ben*

Forráscím	Célcím	Kulcsfelügyeleti (SKIP-) fejléc	Hitelesítési fejléc	Beágyazott tartalom
Beágyazott csomag				

2. ábra: Beágyazott IPSec-csomag

3. ábra: Megosztott titkos adat generálása Diffie-Hellman módszerrel



definiált módon), 160 bites kulcsolt SHA1-gyel (az RFC 1852-ben definiált módon), vagy 160 bites HMAC-SHA1-gyel (az RFC 2104-ben definiált módon). A hitelesítési fejléc ezenfelül tartalmaz adatokat a célból, hogy a fogadó ellenőrizhesse az adatok integritását, azt, hogy nem sérült-e a csomag továbbítás közben.

- *Encapsulated Security Payload (ESP)* (az RFC 1827-ben definiálva). Az eredeti IP- (vagy IPX-) csomag adatait titkosítja az alábbi 4 szabványos titkosítási algoritmus valamelyikével: RC5-CBC (az RSA által definiált módon), RC2-CBC (az RSA által definiált módon), DES-CBC (az RFC 1829-ben definiált módon), vagy Triple DES-CBC (az RFC 1851-ben definiált módon). A titkosítás biztosítja az adatok titkosságát.

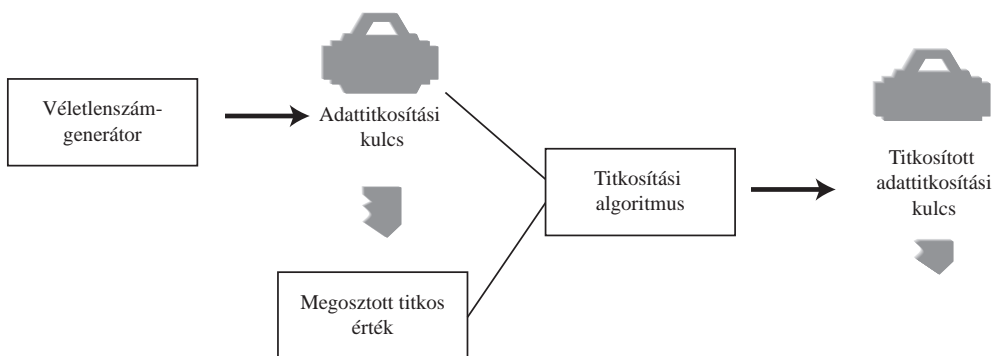
A BIZTONSÁGI KULCSOK FELÜGYELETE

A Sun Microsystems által definiált SKIP egy feltörekvő szabvány az Internet egyes entitásai közötti titkosítási kulcsok felügyeletére. Ez a protokoll titkos, kétirányú kommunikációt tesz lehetővé az Interneten ún. inline- (vonali) kulcscserét használva.

A protokoll vázlatosan a következő módon működik a VPN-szerverek (ill. a kliens és a szerver) között:

Mindkét szerver elvégéz egy bizonyos speciális számítást a Diffie-Hellman algoritmussal. (Ld. 3. ábra.) Mindkét szerveren ugyanazon paraméterekkel kell lefuttatni a Diffie-Hellman algoritmust. Ez úgy oldható meg, hogy a szerverek rendszergazdái előzőleg megosztják egymással a paramétereiket a titkos csatornától független módon, például titkosított e-mailben. Az algoritmus során mindkét szerver saját privát Diffie-Hellman értékét, valamint a másik szerver nyilvános Diffie-Hellman értékét használja fel. A számítás eredménye a két szerver közötti „megosztott titoknak" (shared secret) számít. Ezt a titkos értéket a szerverek időről időre újraszámítják a biztonság növelése érdekében.

Amint a 4. ábrán látható, egy véletlenszám-generátor segítségével mindkét szerver készít egy titkosítási kulcsot, és ezt a kulcsot használja a VPN-en keresztülhaladó csomagok titkosításához és visszafejtéséhez. Mindkét szerver a megosztott titkos értéket



4. ábra: az adattitkosítási kulcs generálásának folyamata

használja a titkosítási kulcs titkosításához, és a kulcsot a csomagokkal együtt küldi el a másik szervernek, minden egyes csomagban.. Az adattitkosítási kulcs n csomagonként változik, a biztonság növelése érdekében. (n értékét a VPN-rendszergazda határozza meg.)

A fogadó szerver ezek után visszafejti az adattitkosítási kulcsot, annak segítségével ellenőrzi a csomag hitelességét, majd visszafejti magát a csomagot. A szerver ezután a visszafejtett csomagot a megfelelő fogadóhoz továbbítja.

BORDERMANAGER VPN SERVICES 3

A Novell BorderManager VPN Services 3 átfogó VPN-megoldást kínál, amellyel biztonságosan és gazdaságosan alakíthatók ki magánhálózatok az Interneten vagy a vállalati intraneten. A BorderManager VPN Services 3 kezeli az IP és IPX protokollokat egyaránt – ezzel egyedül áll a piacon. A BorderManager VPN Services 3 szorosan összeépül az NDS-sel, a VPN felügyeletének

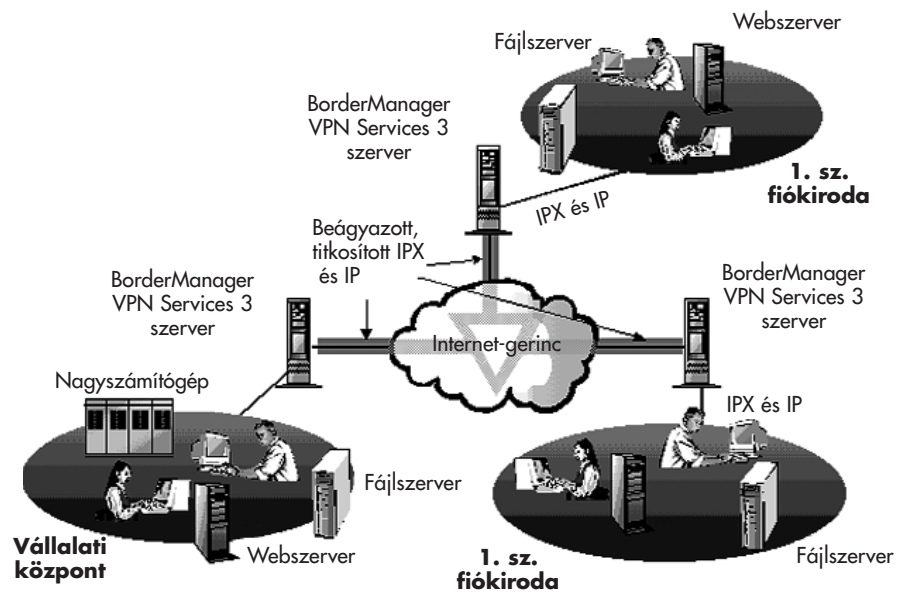
és üzemeltetésének leegyszerősítése érdekében.

A BorderManager VPN Services 3-mal készíthető mind telephelyek közötti, mind kliensek és telephelyek közötti VPN-ek. A BorderManager VPN Services 3 igen jól méretezhető, képes akár alagutanként 256 telephelyet, illetve szerverenként 1000 behívó felhasználót kiszolgálni. Ezenfelül a BorderManager VPN Services 3 kezeli a szimmetrikus többfeladatos rendszereket a nagyobb sebesség érdekében.

TELEPHELYEK KÖZÖTTI VPN

Telephelyek közötti BorderManager VPN Services 3 VPN-t létrehozva a független LAN-szegmensek egyetlen összetartozó nagytávolságú hálózattá egyesíthetők az Internetet használva távolsági kapcsolatként. Mivel a BorderManager VPN Services 3 az IP és IPX protokollokat egyaránt kezeli, a LAN-szegmensek szintén állhatnak IP- és IPX-hálózatok tetszés szerinti kombinációjából.

**5. ábra: Telephelyek közötti
BorderManager VPN**



Az 5. ábrán látható módon, a telephelyek közötti VPN létrehozásához az összes telephelyen létre kell hozni egy BorderManager VPN Services 3 szervert, és össze kell kötnünk őket az Interneten keresztül. A szerverek kapcsolódhatnak háló, gyűrű vagy csillag konfigurációban.

Használható a telephelyek közötti VPN-konfiguráció arra is, hogy egy, a vállalati hálózatot az üzleti partnerek hálózatával összekötő extranetet alakítsunk ki. Az egyetlen különbség az extranet és a cég saját telephelyek közötti VPN-je között a BorderManager VPN Services 3 szerverek fizikai helye.

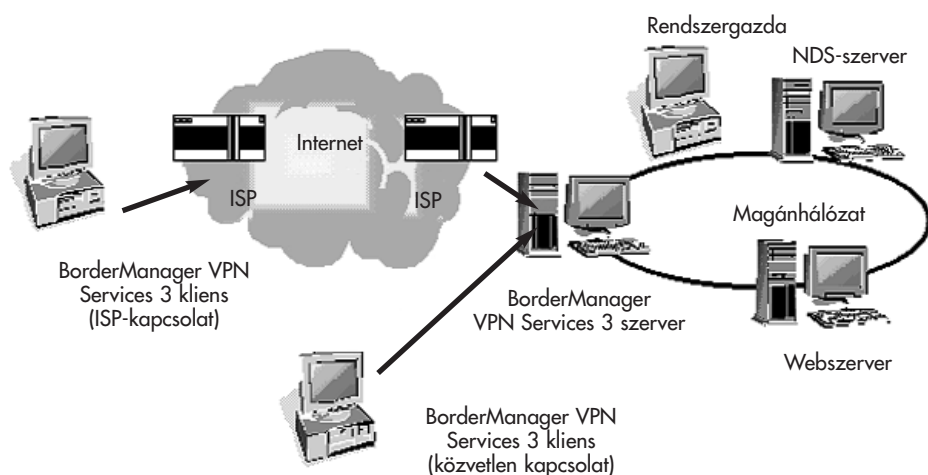
KLIENS ÉS SZERVER KÖZÖTTI VPN

Kliens–szerver VPN-t létrehozva a BorderManager VPN Services 3-mal megoldható, hogy a távoli, telefonon keresztül behívó felhasználók biztonságos

internetes kapcsolaton keresztül férhessenek hozzá a VPN-erőforrásokhoz (ld. 6. ábra.) Ily módon gazdaságos és biztonságos hozzáférés alakítható ki a távoli felhasználók számára, mindazon erőforrásokhoz, amelyekre csak szükségük van, függetlenül az ok vagy az erőforrások helyétől.

A felhasználók a VPN-t a BorderManager VPN Services 3 kliensen keresztül érik el. A kliens a BorderManager VPN Services 3 szerverre csatlakozik, amelyik átjáróként funkcionál a VPN felé. A felhasználó kapcsolódhat a VPN-szerverhez PPP-n, egy Internet-szolgáltatón keresztül, de kapcsolódhat közvetlenül is egy távoli hozzáférési programmal, mint például a NetWare Connect.

Az optimális teljesítmény biztosítása érdekében a BorderManager VPN Services 3 kliens beállítható úgy, hogy csak a – rendszergazda által meghatározott – védett hálózatok adatforgalmát titkosítsa.



6. ábra: BorderManager kliens-szerver VPN

ARCHITEKTÚRA

A BorderManager VPN Services 3 szabványalapú, a Novell-címtárszolgáltatáshoz (NDS-hez) szorosan illeszkedő modern architektúrára épül. Ez a felépítés maximális rugalmasságot biztosít, egyszerűsíti a VPN-ek üzemeltetését és felügyeletét, valamint lehetővé teszi, hogy a felhasználók egyetlen bejelentkezéssel hozzáférjenek az összes hálózati erőforráshoz.

SZABVÁNYALAPÚSÁG

A BorderManager VPN Services 3 kezeli az összes fontos szabványos alagútkezelési, titkosítási és kulcsfelügyeleti mechanizmust, így erős, ugyanakkor rugalmas biztonsági keretrendszert képes nyújtani. Kezeli a gyakorlatban is bizonyított IPSec szabványra épülő alagútkezelést. Kezeli a kulcsok kezelésére szolgáló SKIP szabványt. S végül kezeli a továbbított adatok szabványos transzformációit: mind az USA-belföldi, mint a nemzetközi programváltozat képes használni a 128 bites kulcsolt MD5-öt, a 128 bites HMAC-MD5-öt, a 160 bites kulcsolt SHA1-et és a 160 bites HMAC-SHA1-et.

A BorderManager VPN Services 3 ezenfelül kezeli az megosztott titkos kulcskezelési és adattitkosítási szabványokat is. Az USA-belföldi változat a 128 bites RC2-CBC, a 128 bites RC5-CBC, a 64 bites DES-CBC és a 192 bites TripleDES-CBC kulcs/adattitkosítást képes használni. Az exportváltozat a 64 bites RC2-CBC és a 64 bites RC5-CBC kulcsitkosítási, valamint a 40 bites RC2-CBC és a 40 bites RC5-CBC adattitkosítási szabványokat kezeli.

NDS-INTEGRÁCIÓ

A BorderManager VPN Services 3 az összes felhasználót az NDS-en keresztül hitelesíti, így biztosítva, hogy kizárólag a szigorúan meghatározott VPN-közösség tagjai használhassák a VPN-t. A rendszergazdák a VPN-hez való hozzáférést egyszerűen a felhasználó az NDS-ben tárolt ún. hozzáférés-vezérlési listáján (ACL-jén) keresztül szabályozhatják. Más szavakkal, a VPN-felhasználók pontosan ugyanazon NDS-adatbázissal felügyelhetők, mint minden más hálózati felhasználó. Nem szükséges külön adatbázist fenntartani a VPN-felhasználók számára, s így egyszerűsíthető a felügyelet.

A BorderManager VPN Services 3 három új tulajdonsággal bővíti az NDS NetWare Control Protocol (NCP) szerverobjektumot:

- *A védett hálózatok listája.* A lista minden egyes eleme az adott VPN-szerver által védett hálózat címét és alhálómaszkját határozza meg.
- *Védett hálózatok jelzőbit.* Egyetlen érték, amelyik azt határozza meg, hogyan titkosítják az IP-adatokat az ehhez a VPN-szerverhez kapcsolódó VPN-kliensek. Az érték az alábbiak valamelyike lehet: minden IP-forgalmat titkosít; egyáltalán nem titkosít; csak az adott szerver védett hálózatainak forgalmát titkosítja. (Az IPX-forgalom mindig titkosítódik, függetlenül a jelzőbit értékétől.)
- *VPN-kliens inaktivitásának határértéke.* Egy olyan egyértékű tulajdonság, amely azt határozza meg, hogy a kliens milyen mértékű inaktivitása után bontsa az adott VPN-szerver a kliens kapcsolatát.

A BorderManager VPN Services 3 által a NetWare Administrator-hoz telepített bedolgozómodul automatikusan létrehozza ezeket az attribútumokat mindazon NCP-szerverek esetében, amelyek VPN-szerverekként is működnek, és alapértelmezésű értékekkel tölti fel őket.

TELEPHELYEK KÖZÖTTI VPN KIALAKÍTÁSA BORDERMANAGER VPN SERVICES 3-MAL

A BorderManager VPN Services 3-mal egy cég különálló hálózati szegmensei egyetlen, nagytávolságú hálózattá foghatók össze.

TELEPÍTÉS ÉS BEÁLLÍTÁSOK

Telephelyek közötti VPN esetében a BorderManager VPN Services 3 szervereket master/slave (alá- és fölérendelt) viszonyra kell beállítani, felügyeleti okokból. A teljes VPN központilag, a master szerverről konfigurálható és felügyelhető. Ez leegyszerűsíti a hálózatfelügyeletet és az üzemeltetést.

Rendkívül egyszerű a telephelyi VPN kialakítása a BorderManager VPN Services 3-mal. Elsőként a BorderManager VPN Services 3 master szervert kell telepíteni, az alábbi lépések szerint:

- *Telepítsük a BorderManager VPN Services 3-at a master szerverre. (A legelső szerver lesz a master szerver.)*
- *Generáljuk le a master szerveren a fő (master) RSA privát/nyilvános kulcspárt.*
- *Generáljuk le a master szerver Diffie-Hellman nyilvános és privát kulcsait.*
- *Küldjük át a fő RSA nyilvános kulcsot és a master szerver Diffie-Hellman paramétereit – amelyekkel a master szerver Diffie-Hellman nyilvános és privát kulcsait generáltuk – az összes alárendelt (slave) gépnek. (Ez jellemzően valamilyen sávonkívüli módszerrel, általában titkos e-mailben keresztül történik.)*

Következő lépésként a rendszergazda telepíti és konfigurálja a BorderManager VPN Services 3-at az összes alárendelt szerveren, az alábbi lépések szerint:

- *Telepítsük a BorderManager VPN Services 3-at az alárendelt (slave) szerverre.*
- *Generáljuk le az alárendelt szerver Diffie-Hellman nyilvános és privát kulcsait ugyanazokkal a Diffie-Hellman paraméterekkel, amelyeket e-mailben kaptunk a master szerver rendszergazdájától.*

- *Tároljuk az alárendelt szerveren a master szerver RSA nyilvános kulcsát, amelyet e-mailben kaptunk a master szerver rendszergazdájától.*
- *Küldjük el az alárendelt szerver Diffie-Hellman nyilvános kulcsát a master szerver rendszergazdájának. (Ez jellemzően valamilyen sávonkívüli módszerrel, általában titkos e-mailen keresztül történik.)*

Ha már legalább egy alárendelt szerver működik, akkor a VPN már konfigurálható a master szerverről, az alábbi módon:

- *Válasszuk ki a gyűrű, háló vagy csillag konfigurációt.*
- *Válasszuk ki a használni kívánt titkosítási és hitelesítési módszert.*
- *Válasszuk ki az alagúton keresztül továbbítani kívánt protokollokat (IP, IPX vagy mindkettő).*
- *Határozzuk meg az adattitkosítási kulcs váltási idejét (csomagok számában).*
- *Engedélyezzük vagy tiltsuk le a dinamikus útválasztást.*

A master szerver rendszergazdája ezután begyűjti az alárendelt szerverek rendszergazdáitól az alárendelt szerverek Diffie-Hellman nyilvános kulcsértékeit, majd szétosztja ezeket és a master Diffie-Hellman nyilvános kulcsértékét az összes többi (slave) szerverre. A master szerver a csomagokat a saját RSA privát kulcsával írja alá. Minden egyes alárendelt szerver a megkapott Diffie-Hellman nyilvános értékeket a korábban sávon kívül megkapott master RSA nyilvános kulccsal ellenőrzi.

A master szerver ezután elküldi a VPN konfigurációs adatait az összes többi szervernek. Meghatározza a virtuális hálózat topológiáját (csillag, háló vagy gyűrű), azt, hogy mely protokollokat kell

beágyazni (IP, IPX vagy mindkettő), a híváskezdeményezési módszert, valamint a statikus útvonalakat (amennyiben ezeket állítottuk be). A master szerver az összes elküldött konfigurációs csomagot aláírja.

ALAGUTAK AUTOMATIKUS LÉTREHOZÁSA

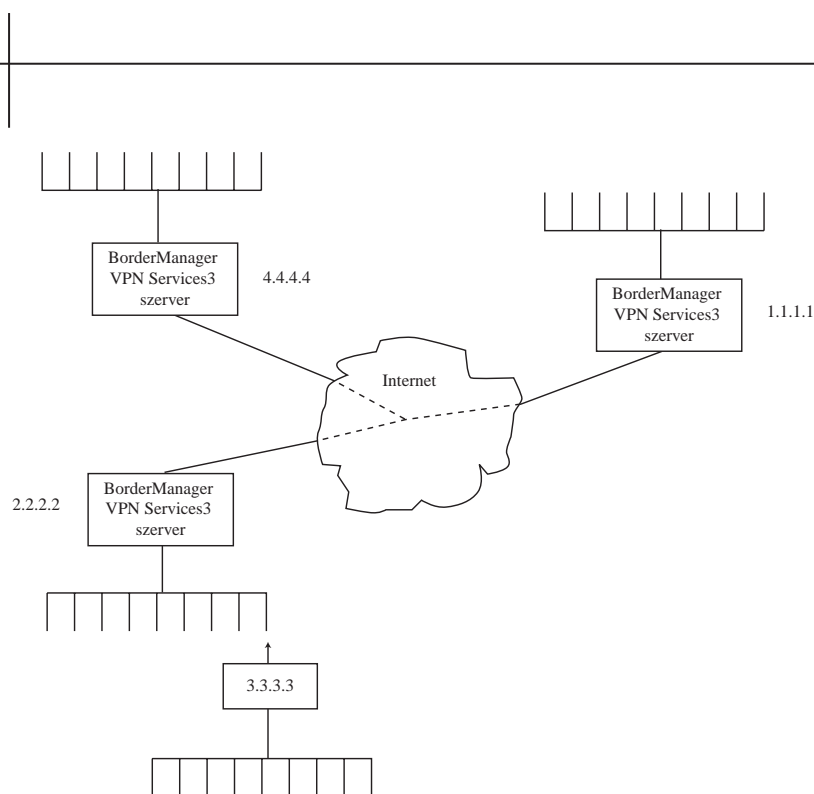
A master és az összes alárendelt szerver telepítése és beállítása után a VPN-szerverek automatikusan létrehozzák az alagutakat: automatikusan hívásokat kezdeményeznek egymás felé. A VPN-szerverei kétféle híváskezdeményezési módra állíthatók be: (1) vagy minden másik VPN-szerver felé kimenő hívást kezdeményeznek, vagy (2) csak azon VPN-szerverek felé kezdeményeznek VPN-hívásokat, amelyek maguk nem hívják az adott szervert. Az alagút létrejötte után addig nem is bomlik le, amíg manuálisan meg nem szüntetik, vagy a VPN-szervert le nem kapcsolják..

Amennyiben a VPN-szerver bármilyen oknál fogva kikapcsolódik, a visszakapcsolás után automatikusan újra létrehozza az összes olyan VPN-szerver felé az alagutakat, amelyekhez korábban kapcsolódott. A híváskezdeményezési mód (bejövő, kimenő vagy mindkettő) a beállításoktól függ.

DINAMIKUS ÚTVÁLASZTÁS

Amennyiben új hálózatot veszünk fel egy már védett hálózatba bármelyik VPN-szerveren, a többi VPN-szerver automatikusan megtanulja az új hálózat címét, és felveszi azt az útválasztási táblába – más szavakkal, a BorderManager VPN Services 3 képes dinamikus útválasztásra. A rendszergazdának nem kell kézzel konfigurálnia a hálózatot minden egyes VPN-szerveren.

**7. ábra: Automatikus
útválasztás**



Ha például felvesszük a 3.3.3.3 hálózatot a 2.2.2.2 című VPN-szerver mögötti védett hálózatra a 7. ábrán látható módon, akkor az 1.1.1.1 és 4.4.4.4 VPN-szerverek automatikusan megtanulják, hogy a 3.3.3.3 hálózat csomópontjait a 2.2.2.2 VPN-szerveren keresztül kell elérniük.

Amennyiben kívánjuk, a dinamikus útválasztás letiltható.

KLIENS ÉS TELEPHELY KÖZÖTTI VPN KIALAKÍTÁSA BORDERMANAGER VPN SERVICES 3-MAL

A BorderManager VPN Services 3-mal készült kliens–telephely VPN egy BorderManager VPN Services 3 szerverből, valamint egy vagy több BorderManager VPN Services 3 kliensből áll. A BorderManager VPN Services 3 kliens Windows 95/98 alatt fut, és szervesen összeépül a Windows telefonos hálózatával. A BorderManager VPN Services 3 kliens a

Novell klienssel integrált bejelentkezést biztosít, így a felhasználó egyetlen bejelentkezéssel hozzáfér az összes hálózati erőforráshoz.

Bármelyik BorderManager VPN Services 3 szerver képes VPN-átjáróként működni a BorderManager VPN Services 3 kliensek számára. Ugyanez a szerver egyidejűleg képes telephelyek közötti master vagy alárendelt szerverként funkcionálni. A VPN-átjárószerver titkosított alagutat biztosít a VPN-kliensek számára, amelyen keresztül biztonságosan tudnak kommunikálni a szerver által védett hálózatokkal.

A BorderManager VPN Services 3 szerverhez kapcsolódó kliensek hozzáférését az adott szerver rendszergazdája szabályozza, az NDS hozzáférés-vezérlési listáján keresztül.

**AUTOMATIKUS KONFIGURÁCIÓ ÉS ALAGUTAK
KIALAKÍTÁSA**

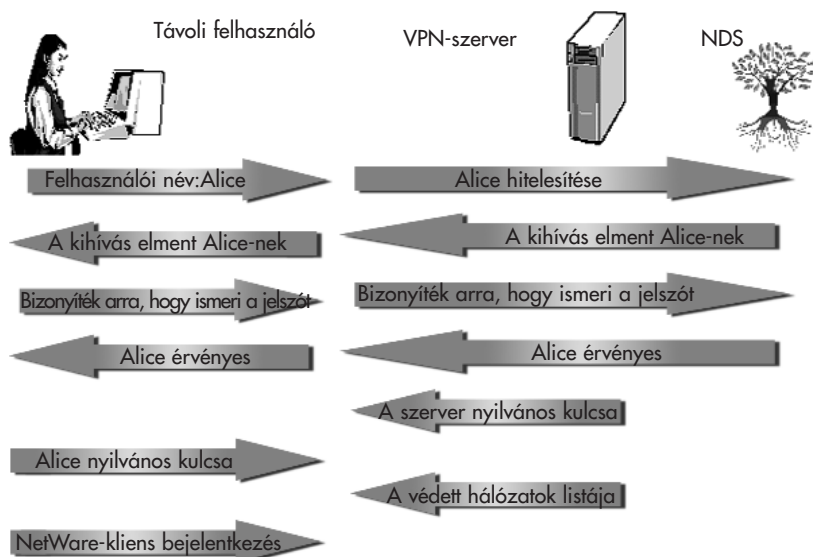
A BorderManager VPN Services 3 kliens automatikusan kialakítja az átjárószerver felé az alagutat. Ez a kliens–telephely alapú működésnél azért fontos, mert új alagutat kell minden egyes kapcsolathoz létrehozni.

A kapcsolat kezdeményezésekor a BorderManager VPN Services 3 kliens a Windows 95/98 telefonos hálózatát használva távoli PPP-kapcsolatot kezdeményez akár egy Internet-szolgáltató, akár közvetlenül a BorderManager VPN Services 3 szerver felé. Ez utóbbi esetben be kell kapcsolni a Novell Internet Access Server (NIAS) távoli hozzáférési funkcióját a szerveren.

A PPP-kapcsolat létrehozása után a BorderManager VPN Services 3 kliens az NDS-en keresztül, egy ún. „kihívásos válasz”- (challenge response) mechanizmussal hitelesíti magát a VPN-átjárószerverhez (ld. 8. ábra).

A „kihívásos válasz”-elvő hitelesítési folyamat lépései az alábbiak:

1. A felhasználó bejelentkezik a saját felhasználói azonosítójával és jelszavával.
2. A kliens csak a felhasználó nevét küldi el a szervernek. (A jelszó biztonsági okokból nem továbbítódik a dróton keresztül.)
3. A VPN-szerver megkeresi a felhasználó adatait tároló NDS-szervert.
4. A VPN-szerver ellenőrzi az NDS-en keresztül, hogy a felhasználó valóban jogosult-e hozzáférni-e az adott VPN-szerverhez. (E ponttól kezdve a VPN-szerver az NDS-szerver proxyjaként működik. A hitelesítési folyamatot ténylegesen az NDS-szerver végzi.)
5. Az NDS-szerver kiszámít egy „kihívásos válasz”-értéket a felhasználó eltárolt jelszava alapján, és visszaküldi azt a klienshez a VPN-szerveren keresztül. (A



**8. ábra. A kihívásos
válaszon alapuló hitelesítés**

VPN-szerver ezt a csomagot a saját RSA nyilvános kulcsával titkosítja a hitelesítés érdekében.)

6. Amennyiben ez a kliens első bejelentkezése az adott VPN-szerverre, úgy megjelenik egy párbeszédablak, ahová a felhasználónak be kell írnia a VPN-szerver RSA nyilvános kulcsát. Ezt a felhasználó a szerver rendszergazdájától kapja meg (jellemzően e-mailben). Helyesen megadva a 16 bájtos értéket, a kliens elmenti azt, és a további hitelesítések automatikusan történnek mindaddig, amíg a kulcsot újra nem generálja a VPN-szerver. (Ezt időről időre célszerű megtenni biztonsági okokból.)

7. A kliens kiszámítja egy másik „kihívásos válasz”-értéket a jelszó és az NDS-szervertől kapott véletlen érték alapján, majd visszaküldi azt az NDS-szerverhez a VPN-szerveren keresztül.

8. Az NDS-szerver a visszaküldött értékből megállapítja, hogy a kliens helyes jelszót adott-e meg. Amennyiben igen, úgy az NDS-szerver hitelesíti a klienst.

Miután az NDS hitelesítette a klienst, visszaadja az irányítást a VPN-szervernek. A VPN-szerver az RSA nyilvános kulcsával titkosítja és aláírja a VPN konfigurációs adatokat, és elküldi azokat a kliensnek. Ezek között megtalálhatók a VPN-szerver Diffie-Hellman paraméterei, valamint a Diffie-

Hellman nyilvános kulcsértéke. Megtalálhatók továbbá a VPN-szerver beállításai is: a védett hálózatok listája, a védett hálózati jelzőbitje, valamint a többi biztonsági paraméter (például a beállított titkosítási és hitelesítési módszerek).

A kliens a szervertől kapott konfigurációs adatok segítségével automatikusan konfigurálja magát, és létrehoz egy alagutat. A VPN-szerver Diffie-Hellman paraméterei alapján generálja le saját Diffie-Hellman nyilvános és privát kulcsát. A kliens saját Diffie-Hellman nyilvános kulcsát visszaküldi a VPN-szervernek, a kliens RSA privát kulcsával aláírva. A kliens ezután a saját Diffie-Hellman privát kulcsa és a szerver Diffie-Hellman nyilvános kulcsa segítségével készíti el a „megosztott titok” értéket, és létrehozza a VPN-szerver felé az alagutat.

A kliens a szervertől kapott adatok – a védett hálózatok listája és a védett hálózatok jelzőbitje – alapján határozza meg, hogy mely IP-csomagokat kell titkosítani. A jelzőbittel beállítható, hogy csupán az adott VPN-szerver védett hálózatai felé menő IP-csomagokat titkosítsa. (Az IPX-csomagokat mindenképpen titkosítja a kliens, függetlenül a védett hálózatok jelzőbitjének értékétől.) Ez a szelektív titkosítás maximálisra növeli a teljesítményt, hiszen a kliens a nem védett IP-helyszínekhez (például webhelyekhez) titkosítás nélkül férhet hozzá.

VPN		VPN	
állapota		-forgalom	
Szerver IP-címe	141.141.0.1	Küldött titkosított IPX-csomagok száma	212
Helyi IP-cím	141.141.0.1	Fogadott titkosított IPX-csomagok száma	1,342
Aktív idő	5:45	Küldött titkosított IP-csomagok száma	101
Kulcsfelügyelet	SKIP	Fogadott titkosított IP-titkosított	100
Titkosítási típus	a rc5 cbc	Küldött titkosított titkosított	8
Hitelesítés típusa	mdc	Fogadott titkosítatlan csomagok száma	8
Titkosítási kulcs mérete	128 bit	Eldobott küldött csomagok	1
Hitelesítés kulcs mérete	128 bit	Eldobott fogadott csomagok	0
IP-titkosítás engedélyezve	igen	Küldött csomagok összesen	321
IPX-titkosítás engedélyezve	igen	Fogadott csomagok összesen	1,450
Szétkapcsolási időkorlát	auto keep alive	Küldött bájtok összesen	55,274
A szétkapcsolásig maradt idő	auto keep alive	Fogadott bájtok összesen	149,148

OK Tovább Szétkapcsolás

9. ábra: A kliensaktivitás monitorképernyője

A KAPCSOLAT AKTIVITÁSÁNAK FIGYELÉSE

A távoli felhasználó figyelheti a kapcsolatot a kliens aktivitásfigyelő képernyőjén. A 9. ábrán e képernyő látható.

A BORDERMANAGER ENTERPRISE EDITION 3 INTERNETES BIZTONSÁGI FELÜGYELETI CSOMAG RÉSZE

A BorderManager 3 VPN Services 3 a BorderManager Enterprise Edition 3 termékcsoport – egy teljeskörű, integrált biztonsági megoldás – része. A BorderManager 3 VPN Services 3 mellett a BorderManager Enterprise Edition 3 az alábbi termékeket tartalmazza:

- A BorderManager Firewall Services 3 biztonsági irányelvek címtáralapú felügyeletét valósítja meg, a bizalmas adat védelme, valamint a felhasználók az intranetes és Internetes tartalomhoz való

hozzáféréseinek vezérlése céljából.

- A BorderManager Authentication Services 3 lehetővé teszi, hogy a felhasználók távolról, behívással, az Interneten keresztül csatlakozzanak a hálózathoz és férhessenek hozzá az összes szükséges hálózati erőforráshoz – alkalmazáshoz, fájlhoz, nyomtatóhoz és szolgáltatáshoz –, mindössze egyetlen jelszóval..
- A BorderManagerFastCache™ Services 3 az iparág leggyorsabb, legjobban méretezhető internetes gyorsítótár-szolgáltatása, minden webet is használó cég, tartalom- és Internet-szolgáltató számára.
- A NetWare® 5 egy teljeskörű, az NDS-t kihasználó megoldás biztosítása érdekében.

NDS-INTEGRÁCIÓ

A BorderManager Enterprise Edition 3 a Novell-címtárszolgáltatást (NDS-t) kihasználva az alábbi funkciókat képes nyújtani:

- Átfogó, nagyteljesítményű intranetes és Internetes védelem. A kiváló tűzfal-, gyorsítótár-, távoli hitelesítési és VPN-technológiákkal nagyteljesítményű, globális, nemcsak a külső, hanem a belső támadásoktól is védett vállalati hálózatok alakíthatók ki.
- Az irányelvek címtáralapú felügyelete. Mivel a BorderManager Enterprise Edition 3 szorosan egybeépül az NDS-sel, a hálózati rendszergazdák egyetlen, központi helyről szabályozhatják a biztonsággal és a hozzáféréssel kapcsolatos összes kérdést, lényegesen csökkentve ezáltal a felügyelet bonyolultságát. Hogy mennyire? A felmérések szerint akár 70 százalékkal.
- Valódi egyponthus bejelentkezés a hálózati szolgáltatásokra. Az NDS-en keresztüli egyetlen bejelentkezéssel a felhasználók hozzáférhetnek az összes hálózati erőforrásukhoz, függetlenül attól, hogy hol léptek be a hálózatba, vagy attól, hogy pontosan hol is található az erőforrások. A biztonsági irányelvek betartatása a felhasználók számára láthatatlanul zajlik, ezzel is növelve a felhasználók termelékenységét.
- Bővíthető keretrendszer. A BorderManager Enterprise Edition 3-mal a cégek a biztonsági szolgáltatásokat üzleti igényeiknek megfelelő sebességgel telepíthetik – vagyis folyamatosan

kihasználhatják meglévő befektetéseiket.

ÖSSZEFOGLALÁS

A virtuális magánhálózatok (VPN-ek) ideális megoldást kínálnak minden olyan szervezet számára, akik több telephelyet egyetlen hálózattá kívánnak szervezni, illetve akik hálózati hozzáférést kívánnak nyújtani a távoli, telefonon keresztül behívó felhasználók számára. Mivel a VPN-ek az Internetet vagy a vállalati intranetet használják kapcsolati médiumként, sokkal gazdaságosabbak, mint a drága egyedi bérelt vonalak és az azokhoz tartozó speciális berendezések. VPN használata esetén nincsen szükség sem modemfarmok, sem a távoli felhasználók hozzáférését biztosító egyéb speciális berendezések vásárlására és üzemeltetésére sem.

A Novell BorderManager Enterprise Edition 3 igen vonzó VPN-megoldást kínál. Lehetővé teszi mind a telephelyek közötti, mint kliensek és telephelyek közötti VPN-ek kialakítását. Képes kezelni az IP- és IPX-hálózatokat egyaránt. Ismeri és kezeli az összes VPN-szabványt. Rendkívül jól méretezhető. Egybeépül az NDS-sel a VPN felügyeletének és üzemeltetésének leegyszerűsítése érdekében. S végül, de nem utolsósorban a termék mögött a Novell áll, a világon több mint félmillió oktató és tanácsadó szakemberével.

A BorderManager Enterprise Edition 3 VPN-nel szorosabb együttműködés alakítható ki az alkalmazottakkal és az üzleti partnerekkel, és növelhető a cég kompetitív előnye.

Novell Corporate Headquarters

122 East 1700 South
Provo, UT 84606
USA
Tel: (801) 861 7000
Toll-free: (800) 453 1267

AMERICAS REGION**Novell Canada**

3100 Steeles Avenue East
Suite 500
Markham, Ontario L3R 8T3
Canada
Tel: (905) 940 2670
Fax: (905) 940 2688

Novell de Argentina

Av. Leandro N. Alem 1110 9°
1001 Buenos Aires
Argentina
Tel: (54) 11 4 312 2626
Fax: (54) 11 4 312 8025

Novell Bolivia

One East Broward Blvd.
Barnett Bank Plaza, Suite 700
Ft. Lauderdale, FL 33301
Tel: (954) 713 2869
Fax: (954) 356 0409

Novell do Brasil Software Limitada

Avenida das Nações
Unidas, 12.995
8° Andar
04578-000 São Paulo - SP
Brazil
Tel: (55) 11 5505 4040
Fax: (55) 11 5505 4041

Novell Central America, Caribbean, Puerto Rico

One East Broward Blvd.
Barnett Bank Plaza, Suite 700
Ft. Lauderdale, FL 33301
Tel: (954) 713 2869
Fax: (954) 356 0409

Novell de Chile

Av. Nueva Tajamar 555
Of. 901
Las Condes - Santiago
Chile
Tel: (56) 2 3397 070
Fax: (56) 2 3397 071

Novell de Colombia

Teleport Business Park
Calle 114 No. 9 - 45
Torre B - Of. 709
Santafé de Bogotá
Colombia
Tel: (57) 1 629-2969
Fax: (57) 1 629-3509

Novell de Mexico

Bldv. Manuel Avila
Camacho #138-1
Col. Lomas de Chapultepec
Mexico D.F., C.P. 11000
Tel: (52) 5 284 2700
Fax: (52) 5 284 2799

Novell Peru

Martir Olaya 129 Office 1701
Centro Empresarial Pardo
Miraflores
Lima, Peru
Tel: (511) 214 1340
Fax: (511) 214-1087

Novell de Venezuela

Plaza la Castellana
Torre Bancaracas
Piso 10, Ofic.10-04
La Castellana
Codigo Postal 1060
Caracas
Venezuela
Tel: (58) 2 264 2534
Fax: (58) 2 264 2171

EUROPE, MIDDLE EAST, AFRICA REGION**Novell Austria**

Heiligenstädter Lände 27c
1190 Wien
Austria
Tel: (43) 1 36 77 444
Fax: (43) 1 36 77 444 20

Novell Belgium NV

Koningin Astridplein 1,
(3rd floor)
2018 Antwerpen
Belgium
Tel: (32) 3 206 1793
Fax: (32) 3 206 1799

Novell Praha s.r.o.

Praha City Center
Klimentska 46
110 02 Praha 1
Czech Republic
Tel: (420) 2 2185 6611
Fax: (420) 2 2185 6622

Novell Danmark

Slotsmarken 12
DK 2970 Hørsholm
Denmark
Tel: (+45) 45 16 00 20
Fax: (+45) 45 16 00 40

Novell Finland

Sinimäentie 10 C
02630 Espoo
Finland
Tel: (358) 9 502 951
Fax: (358) 9 5029 5300

Novell France

Tour Framatome
1 Place de la Coupole
92084 Paris La Défense
Cedex
France
Tel: (33) 1 47 96 60 60
Fax: (33) 1 47 78 94 72

Novell Germany

Monschauer Strasse 12
40549 Düsseldorf
Germany
Tel: (49) 211 5631 0
Fax: (49) 211 5631 250

Novell Hungary

East-West Business Center
1088 Budapest
Rákóczi út 1-3
Hungary
Tel: (36) 1 235 7656
Fax: (36) 1 266 6360

Novell Israel

Ackerstein Building
Medinat Hayehudim St 103
Herzliyya 46776
Israel
Tel: (972) 99 51 44 55
Fax: (972) 99 51 44 66

Novell Italia

Piazza Don Mapelli 75
20099 Sesto San Giovanni
Milan
Italy
Tel: (39) 02 2626 3262
Fax: (39) 02 2626 3195

Novell Middle East

17th Floor
Dubai World Trade Center
P.O. Box 9313
Dubai
United Arab Emirates
Tel: +971 4 316444
Fax: +971 4 319248

Novell Netherlands

Barbizonlaan 25
2908 MB Capelle a/d IJssel
PO Box 85024
3009 MA Rotterdam
The Netherlands
Tel: (31) 10 286 4722
Fax: (31) 10 286 4010

Novell Norge

Grensesvingen 9
Postboks 6555, Etterstad
0606 Oslo
Norway
Tel: +47 22 08 77 70
Fax: +47 22 08 77 71

Novell Polska

ul. Sienna 64
00-825 Warszawa
Poland
Tel: (48) 22 620 39 79
Fax: (48) 22 620 31 03

Novell Portugal

Regus Business Centre
Centro Empresarial Torres
de Lisboa
Rua Tomas da Fonseca,
Torre G
1600 Lisboa
Portugal
Tel: +351 1 723 06 30
Fax: +351 1 722 35 33

Novell Russia and CIS

Suite 524
Radisson-Slavianskaya Hotel
2 Berezhkovskaya Nab.
Moscow 121059
Russia
Tel: (7) 095 941 8075/73
Fax: (7) 095 941 8066

Novell South Africa

Morning View Office Park
214 Rivonia Road,
Morningside
P.O. Box 1840
Rivonia 2128
Gauteng
Republic of South Africa
Tel: (27) 11 322 8300
Fax: (27) 11 322 8400

Novell Spain, S.A. (Madrid)

Paseo de la Castellana, 95
27th Floor
Torre Europa
28046 Madrid
Spain
Tel: (34) 91 555 65 67
Fax: (34) 91 555 29 15

Novell Spain, S.A. (Barcelona)

Avda. Diagonal 611.6° A
08028 Barcelona
Spain
Tel: (34) 93 430 47 10
Fax: (34) 93 322 28 90

Novell Sweden

Kronborgsgränd 1
164 87 Kista
Sweden
Tel: +46 8 477 4100
Toll-free: 020 35 3030
Fax: +46 8 477 4101

Novell Schweiz AG

Leutschenbachstrasse 41
8050 Zürich
Switzerland
Tel: (41) 1 308 47 47
Fax: (41) 1 302 04 01

Novell United Kingdom Ltd.

Novell House
1 Arlington Square
Downshire Way
Bracknell
Berkshire, RG12 1WA
United Kingdom
Tel: +44 1344 724000
Fax: +44 1344 724001

ASIA PACIFIC REGION**Novell Pty Ltd**

Level 18, 201 Miller Street
North Sydney NSW 2060
Australia
Tel: +61 2 9925 3000
Fax: +61 2 9922 2113

Novell New Zealand Limited

L12, 44 - 52 Wellesley Street
Auckland 1
New Zealand
Tel: +64 9 308 1400
Fax: +64 9 308 1409

Novell China

Floor 11 Canway Building
No. 66 Nan Li Shi Road
Beijing 100045, China
Tel: (86) 10 68028855
Fax: (86) 10 68028720

Novell Hong Kong

Room 4601-5
China Resources Building
26 Harbour Road
Wanchai
Hong Kong, China
Tel: (852) 2 588 5288
Fax: (852) 2 827 6555

Onward Novell Software (I) Ltd.

62 MIDC, 13th Street
Andheri (East)
Mumbai 400 093
India
Tel: +91 (022) 8342244
Fax: +91 (022) 8342223

Novell Japan Ltd.

Toei Mishuku Bldg.
1-13-1 Mishuku
Setagaya-Ku
Tokyo 154-8561
Japan
Tel: (81) 3 5481 1294
Fax: (81) 3 5481 1934

Novell Korea

Will-Bes Building 11th Floor
942-1, Daechi-dong
Kangnam-ku
Seoul, Korea
135-280
Tel: (82) 2 528 1400
Fax: (82) 2 528 1414

Novell, Inc. Malaysia Representative Office

Unit 501, Level 5, Uptown 1
1 Jalan SS21/58
Damansara Uptown
47400 Petaling Jaya
Selangor Darul Ehsan
Malaysia
Tel: (60) 3 712 6100
Fax: (60) 3 712 6155

Novell Singapore Pte Ltd

300 Beach Road #28-00
The Concourse
Singapore 199555
Tel: (65) 2962866
Fax: (65) 2961266

Novell Taiwan

Rm. E-F, No. 168
Tun-Hwa N. Road
Taipei 105
Taiwan, R.O.C.
Tel: 886-2-2718 9733
Fax: 886-2-2514 9806

Novell, Inc. Thailand Representative Office

Level 23, CP Tower
313 Silom Road
Bangkok
Thailand 10500
Tel: (66) 2 231 8166
Fax: (66) 2 231 8246

© 1999, Novell, Inc. Minden jog fenntartva.
A Novell, a NetWare és a Novell-című szolgáltatás a Novell Corporation bejegyzett védjegye, a BorderManager, a BorderManager FastCache és az NDS pedig védjegyet az Egyesült Államokban és más országokban.

Minden egyéb márka- és terméknév a birtokos cég védjegye vagy bejegyzett védjegye.

A Novell termékfejlesztési és támogatási szolgáltatásai

A Novell az egész világra kiterjedő, a termékekkel kapcsolatos oktatási programjaival, konzultációs és műszaki tanácsadási programjaival kapcsolatos további információ a <http://services.novell.com> címen olvasható.

További információ

Hívja a helyi hivatalos Novell-vizonteladót, vagy látogassa meg a Novell webhelyét a www.novell.hu címen.

USA/Canada: 1-888-321-4272

Egyéb országok: 1-801-228-4272
Fax: 1-801-228-5376

Novell, Inc.

122 East 1700 South
Provo, UT 84606

Novell.