Adatlap

# Cisco ASA 5500 sorozatú berendezések SSL / IPsec VPN kiadás

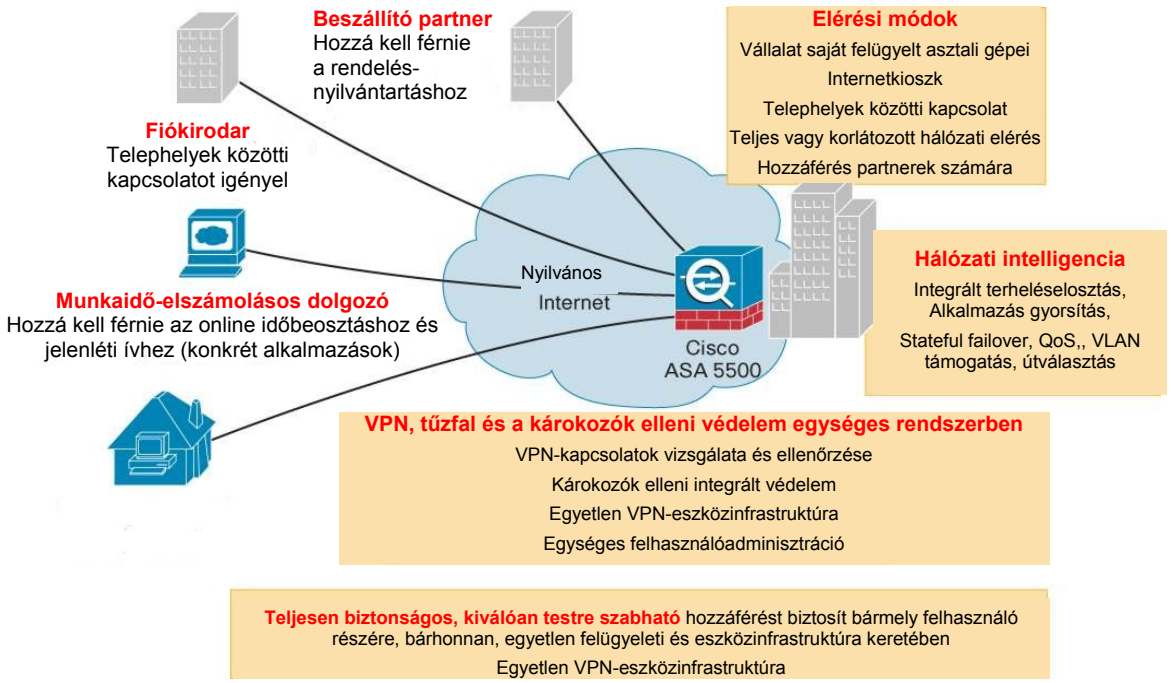
**A Cisco ASA 5500 sorozatú adaptív biztonsági készülék a kis- és középvállalatok hálózataihoz, illetve a nagyobb vállalatok rendszereihez kínál biztonsági szolgáltatásokat és VPN-funkciókat. A sorozatba tartozó készülékek a konkrét működési környezethez igazíthatók, mivel külön termékkiadások álnak rendelkezésre olyan célzott funkciókra, mint a kombinált védelem, az IPS, a tűzfal és a VPN.**

A Cisco ASA 5500 sorozat SSL/ IPsec VPN termékkiadásával a távoli felhasználók vagy telephelyek forgalma az olcsó és könnyen elérhető internetre terelhető anélkül, hogy a vállalat biztonsága csorbát szenvedne. Az SSL és IPsec alapú VPN-szolgáltatásokat átfogó védelmi technológiákkal ötvözve a Cisco ASA 5500 sorozattal tökéletesen testre szabható hálózati hozzáférés alakítható ki, amely sokféle környezetben alkalmazható, ugyanakkor fejlett végponti és hálózati szintű biztonságot nyújt.

## CISCO ASA 5500 SOROZAT: SSL/IPSEC VPN EDITION

A Cisco ASA 5500 sorozat SSL/IPsec VPN kiadás bármely hálózatelérési igénynél rugalmas VPN-hozzáférést biztosít akár 5000 egyidejű felhasználó esetében is. Számos előnyét nehéz lenne mind felsorolni: könnyű felügyelet, teljes csatornás hálózatelérés SSL és IPsec alapú VPN-kliensekkel, fejlett kliensszoftver nélküli SSL VPN, illetve a hálózathoz alkalmazkodó telephelyek közötti VPN-kapcsolat, stb. Segítségével a vállalatok a nyilvános hálózatokon keresztül is biztonságos csatlakozást kínálhatnak a mobil felhasználóknak, a távoli helyszíneken dolgozóknak, alvállalkozóiknak és üzleti partnereiknek (lásd az 1. ábrát). Emellett a Cisco ASA 5500 sorozat SSL/IPsec VPN termékkiadásával csökkenthetők a VPN telepítésének és üzemeltetésének költségei, hiszen a telepítéshez és bővítéshez immár nincs szükség kiegészítő berendezésekre.

**1. ábra** A telepítési környezethez igazítható VPN-szolgáltatások



A Cisco ASA 5500 sorozat SSL/IPsec VPN termékkiadásának előnyei:

- **SSL és IPsec alapú teljes hálózati távelérés** – A hálózati rétegben működő, teljes értékű távoli felhasználói kapcsolatot biztosít gyakorlatilag bármely alkalmazáshoz vagy hálózati erőforráshoz. A hálózatelérést vagy a menet közben letöltött Cisco SSL VPN-kliens, vagy a Cisco IPsec VPN-kliensprogram biztosítja. Általában a felügyelt felhasználói gépekre, így például a vállalat tulajdonában lévő dolgozói laptopokra is kiterjesztik a teljes hálózati hozzáférést. Az SSL és az IPsec alapú távoli eléréses VPN-technológiák támogatása révén a Cisco ASA 5500 sorozatú készülékek különösen rugalmasan működnek, így sokféle telepítési környezetben is tökéletesen kielégítik az igényeket.
- **Kliens nélküli hálózati hozzáférés** – A kliens nélküli távoli hozzáféréssel a hálózati alkalmazások és erőforrások helytől függetlenül, PC-s VPN-kliensszoftver nélkül is elérhetők. A webböngészőkben található, mindenütt jelenlévő SSL-titkosításnak köszönhetően a Cisco ASA 5500 sorozat készülékei kliens nélküli hozzáférést biztosítanak bármilyen webes alkalmazáshoz vagy erőforráshoz, valamint a Citrixhez hasonló terminálszolgáltatásokhoz. Külön optimalizálás szolgája a Microsoft Outlook Web Access és Lotus iNotes hatékony működését, valamint a hozzáférést az olyan gyakori vastagkliens-alkalmazásokhoz, mint az e-mail, az azonnali üzenetküldés, az előjegyzésnaptár vagy a Telnet. Emellett a Cisco ASA 5500 sorozat dinamikus tartalomátszerkesztő képességeivel megbízhatóan renderelhetők a bonyolultabb, Java Script vagy ActiveX kódot tartalmazó weblapok.
- **A hálózathoz alkalmazkodó telephelyek közötti VPN-ek** – Biztonságos, nagysebességű kommunikáció több irodai helyszín között. A teljes VPN-re kiterjedő garantált szolgáltatásminőség (QoS) és útválasztás révén a Cisco ASA 5500 Series SSL/IPsec VPN Edition megbízható, üzleti színvonalú átviteli minőséget biztosít a késleltetésérzékeny alkalmazásokhoz, így a hang- és videoátvitelhez, valamint a terminálszolgáltatásokhoz.
- **Károkozóktól mentes VPN** – A VPN-ek a szervezetek hálózata ellen irányuló rosszindulatú támadások (pl. férgek, vírusok, kémprogramok, billentyűnaplózók, trójai és rootkit programok) elsődleges forrásai. A Cisco ASA 5500 sorozat készülékeibe integrált behatolásmegelőzés, vírusvédelem, alkalmazásfigyelő tűzfal és végponti VPN-biztonsági funkciók segítségével minimálisra csökkenthető annak kockázata, hogy a VPN-kapcsolat kiskaput nyújtson a veszélyforrások számára.
- **Gazdaságosabb VPN-telepítés és üzemeltetés** – A VPN-ek bővítése és biztonságossá tétele kiegészítő terheléselosztó és biztonsági berendezéseket tehet szükségessé, amelyek jelentősen növelhetik a biztonsági és üzemeltetési költségeket. A Cisco ASA 5500 sorozatban ezek a funkciók integráltan találhatók meg, így a mai VPN-termékekhez képest példátlan szintű hálózati és biztonsági integrációt valósítanak meg. Mivel egyetlen platformon egyszerre van lehetőség SSL és IPsec VPN nyújtására, a Cisco ASA 5500 sorozatú készülékek költséghatékony alternatívát kínálnak a párhuzamos VPN-infrastruktúrát telepíteni kívánó ügyfelek számára.
- **Méretezhetőség és hibatűrés –** A készülékek egyszerre akár 5000 egyidejű felhasználói kapcsolatot is kiszolgálnak; ez a szám az integrált fürtözési és terheléselosztási lehetőségek nyomán több tízezerre is növekedhet. Az állapotőrző tartalékaktiválás magas rendelkezésre állást biztosít rendkívül alacsony állásidővel.

## TESTRE SZABHATÓ TÁVOLI ELÉRÉSES VPN-FUNKCIÓK

### Teljes értékű hálózati hozzáférés

A Cisco ASA 5500 Series SSL/IPsec VPN Edition a VPN-csatornát kezelő Cisco SSL VPN vagy a Cisco IPsec VPN kliensen keresztül biztosít széles körű hozzáférést az alkalmazásokhoz és a hálózati erőforrásokhoz.

A Cisco ASA 5500 CSC-SSM szolgáltatásmodul egy sor biztonsági és szabályozási funkcióval rendelkezik, amelyek közül a legfontosabbakat az 1. táblázat szemlélteti.

**1. táblázat** Cisco ASA 5500 sorozat - Teljes értékű hálózatelérés

| Jellemzők | Előnyök |
|---|---|
| **Rugalmas telepítési lehetőségek** | Az egy készüléken megvalósított kettős üzemmódú SSL és IPsec VPN bármely telepítési környezetben teljes értékű távoli hálózatelérést nyújt. |
| **Könnyű kliensadminisztráció** | A Cisco SSL VPN-kliens menet közben töltődik le, így megtakarítható a VPN-kliensszoftver karbantartása<br>A Cisco IPsec VPN-kliens automatikus frissítése rendkívül megkönnyíti a kliensszoftver verziókövetését<br>Az összes felhasználói szabály központilag, egy helyről konfigurálható mind az SSL, mind pedig az IPsec alapú VPN-kliensek esetében<br>Egyszerűbb üzemeltetés a vegyes SSL és IPsec alapú hálózati környezetekben; az egyetlen hardver és az egységes felügyeleti infrastruktúra mindkét felhasználói kör számára előnyös |
| **Egységes környezet** | A teljes csatornás klienseléréssel (mind SSL, mind IPsec esetén) a felhasználó a LAN-nal egyenértékű környezetben dolgozha<br>A Cisco SSL VPN-kliens többféle módon elérhető, és csak kis méretű letöltést igényel. Így számos eszközön pillanatok alatt üzembe helyezhető. |

## Kliens nélküli hálózatelérés

A Cisco ASA 5500 sorozat kliens nélküli SSL VPN-hozzáférése internetes kioszkok, több személy által közösen használt számítógépek, extranetes partnerek, az alkalmazottak saját számítógépei, illetve a vállalati tulajdonú dolgozói számítógépek számára biztosít webes hozzáférést a fontos hálózati erőforrásokhoz és alkalmazásokhoz.

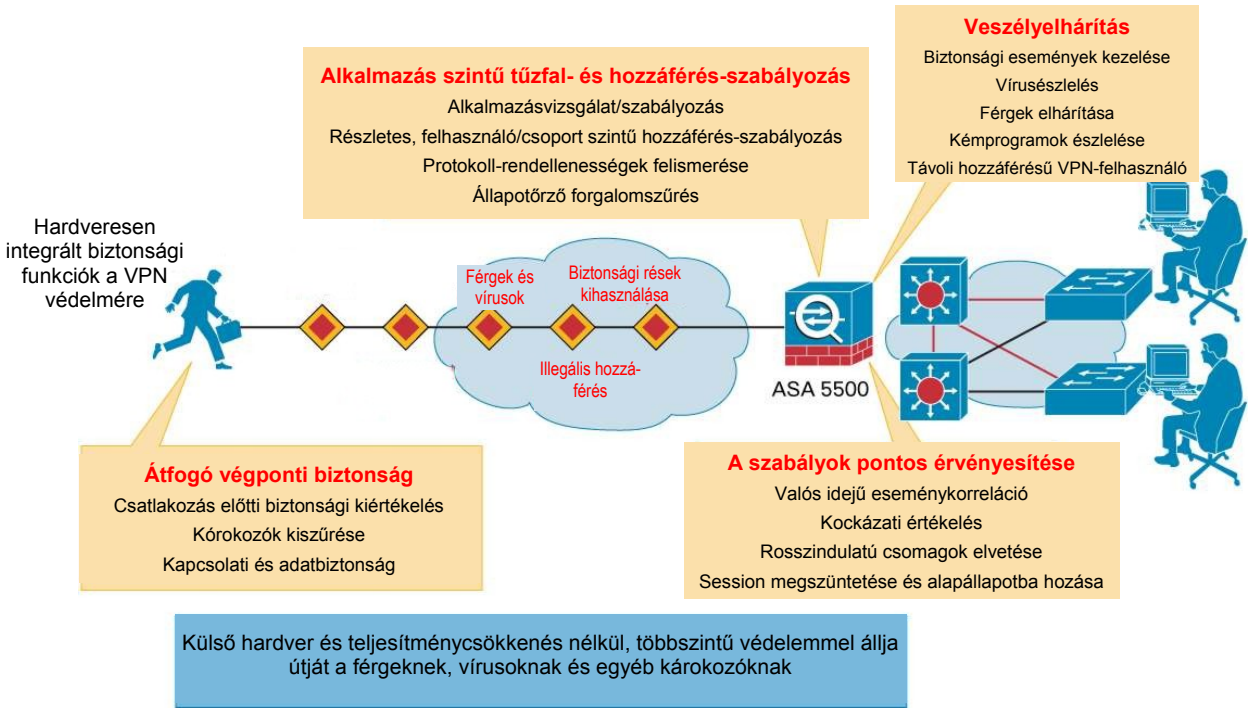
**2. táblázat** Cisco ASA 5500 sorozat - Webes kliens nélküli hozzáférés

| Jellemzők | Előnyök |
|---|---|
| **Széles körű, megbízható kompatibilitás** | A fejlett tartalomszerkesztési funkciókkal a bonyolult HTML, Java, ActiveX és JavaScript kódot tartalmazó weboldalak is könnyen és pontosan kezelhetők |
| **Integrált optimalizálás az alkalmazások kliens nélküli használatához** | Az erőforrás-igényes alkalmazások (mint az Outlook Web Access és a Lotus iNotes) futásteljesítményét optimalizáló beépített funkciók kitűnő válaszidőket és alacsony késleltetést biztosítanak az SSL VPN végfelhasználóinak |
| **Egyedi igényekhez igazítható** | A kliens nélküli elérést szolgáló portálon csoport szintű beállításokkal lehet részletesen szabályozni a hozzáférést, és ki lehet választani a felhasználó munkáját leginkább megkönnyítő beállításokat |
| **Teljesen kliens nélküli Citrix-hozzáférés** | A kliens nélküli SSL VPN-eléréssel megvalósított Citrix-hozzáférés külső nélkül is gyors alkalmazásindítást biztosít, miközben csökkenti a munkahelyi szoftverütközések kockázatát |
| **A gyakori vastagkliens-alkalmazások támogatása** | A porttovábbítás olyan elterjedt vastagkliens-alkalmazásokhoz biztosít kliens nélküli hozzáférést, mint a POP/SMTP/IMAP alapú e-mail, az online naptárak, az azonnali üzenetküldés, a Telnet és más, kliens által indított TCP-alkalmazások |
| **Böngészők széles körű támogatása** | A több böngészőre kiterjedő támogatás (Internet Explorer, Firefox, Opera és Safari) hely-és eszközfüggetlen kompatibilis elérést biztosít |

## A VPN-FUNKCIÓK VÉDELME

A Cisco ASA 5500 sorozatú SSL/IPsec VPN Edition termékkiadás integrált hálózati és végponti biztonsági technológiáival fokozott biztonságot nyújt a VPN-ekhez. A virtuális magánhálózat biztonságossá tétele nélkül a hálózat különféle kórokozók (például férgek, vírusok, kémprogramok, billentyűnaplózók, trójai és rootkit programok vagy kalózbetörések) terjesztési csatornájává válhat. Emellett a VPN-forgalomra részletes alkalmazás szintű és jogosultságkezelési szabályok alkalmazhatók, így az egyéni és csoportos felhasználók csak a számukra engedélyezett alkalmazásokat, hálózati szolgáltatásokat és erőforrásokat érhetik el (2. ábra).

**2. ábra** Hardveresen integrált biztonsági funkciók a VPN védelmére



## Hálózati biztonság a VPN-átjárónál

A férgek, vírusok, alkalmazásokba beágyazott támadások és az alkalmazásokkal való visszaélés manapság a hálózatokat érintő legnagyobb kihívás. A távoli elérés és a távoli helyszínek VPN-kapcsolata a VPN-eszközök korlátozott biztonsági képességei miatt gyakorta kínálnak támadási felületet. A VPN-eket túlságosan gyakran telepítik a központ csatornavégpontjának megfelelő kivizsgálása és kockázatmentesítése nélkül, ami lehetővé teszi, hogy a távoli telephelyekről rosszindulatú programok hatoljanak be a hálózatba és terjedjenek el, vagy jogosulatlan felhasználók kapjanak hozzáférést. A Cisco ASA 5500 sorozat veszélyelhárító funkcióival a rosszindulatú programok észlelhetők, és még azelőtt megállíthatók, hogy bejutnának a belső hálózatba. Az alkalmazásokba ágyazott támadások, mint például a fájlmegosztó P2P-hálózatokon terjedő kém- és reklámprogramok esetében a Cisco ASA 500 sorozatú készülékek alaposan megvizsgálják az alkalmazásforgalmat, hogy kiszűrjék a veszélyes csomagokat, és azok tartalmát még azelőtt letiltsák, hogy elérnének a célpontot és kárt okoznának. A 3. táblázatban a Cisco ASA 5500 sorozat néhány, VPN-átjáró szintű biztonsági funkciója található.

**3. táblázat** Hálózati biztonság a VPN-átjárónál

| Jellemzők | Leírás |
|---|---|
| **Rosszindulatú programok átfogó elhárítása** | A Cisco ASA 5500 sorozatú készülékek a VP-átjárónál torlaszolják el a férgek, a vírusok, a billentyűzetnaplózók, a trójai, a kém- és rootkit-programok útját, megsemmisítve a kározókat, még mielőtt azok továbbterjedhetnének a hálózaton |
| **Alkalmazásokat felismerő tűzfal és hozzáférés-szabályozás** | Az alkalmazásokat felismerő forgalomvizsgálat a felhasználói hozzáférés alapos szabályozását teszi lehetővé, és segít kiszűrni az olyan nem kívánt alkalmazásokat, mint pl. a fájlmegosztók, amelyek a VPN-kapcsolatot is igénybe veszik forgalmukhoz |
| **Behatolásmegelőzés** | A Cisco ASA 5500 sorozatú készülék védi a hálózat számos sebezhető pontját |

## Átfogó végponti biztonság SSL VPN-hálózatokhoz

Az SSL VPN alapú rendszerekkel a biztonságos és a nem vállalatilag felügyelt végpontokról egyaránt egységes hozzáférés biztosítható az eltérő jellegű felhasználói közösségek számára. A hálózat ilyen kibővítésével azonban arányosan nő a hálózat elleni potenciális támadások száma. Függetlenül attól, hogy a felhasználók a hálózathoz egy vállalatilag felügyelt PC-ről, saját számítógépről vagy nyilvános terminálról csatlakoznak, a Cisco Secure Desktop minimálisra csökkenti az SSL VPN-kapcsolatok lezárása után hátramaradt cookie-k, böngésző-előzményadatok, ideiglenes fájlok és letöltött anyagok mennyiségét. A 4. táblázat a Cisco Secure Desktop legfontosabb tulajdonságait ismerteti.

**4. táblázat** Cisco Secure Desktop: Az információk hálózattól végpontig terjedő átfogó biztonsága

| Jellemzők | Leírás |
|---|---|
| **Csatlakozás előtti biztonsági kiértékelés** | A hostgép épségét ellenőrző modul a hálózati hozzáférés engedélyezése előtt átvizsgálja a végponti rendszert, hogy az tartalmaz-e vírusvédelmi szoftvert és személyi tűzfalat, illetve telepítették-e rajta a Windows-javítócsomagokat. |
| **Átfogó kapcsolatvédelem** | Az adott kapcsolattal (session) összefüggő összes adat, köztük a jelszavak, a fájlletöltések, az előzmények, a cookie-k és a gyorsítótár fájljai külön védelmet élveznek. A kapcsolatra vonatkozó titkosított adatok a Cisco Secure Desktop „páncéltermébe” kerülnek. |
| **Adattisztogatás a kapcsolat végén** | A „páncélteremben” őrzött adatok a kapcsolat befejeztével felülíródnak. |
| **A billentyűzetnaplózó programok észlelése** | A Cisco Secure Desktop virtuális asztala minden kapcsolat kezdetén megkísérli felderíteni egyes ismert szoftveres billentyűzetnaplózó eszközök jelenlétét. Ha egy rendellenes viselkedést tanúsító program kezd el futni a „páncéltermen” belül, akkor a felhasználó felszólítást kap, hogy állítsa le a gyanús tevékenységet. |
| **Vendég-hozzáférési jogosultságot is biztosíthat** | A hálózathoz távoli számítógépekről hozzáférő felhasználók feltehetően nem rendelkeznek minden rendszeren rendszergazda jogosultsággal. A Cisco Secure Desktop gyakran csak vendégjogosultsággal telepíthető; ez az összes rendszerre való átvihetőséget és telepíthetőséget szolgálja. |

## A HÁLÓZATHOZ ALKALMAZKODÓ, HELYSZÍNEK KÖZÖTTI VPN

A Cisco ASA 5500 Series SSL/IPsec VPN Edition által biztosított IPsec alapú. a hálózathoz alkalmazkodó, telephelyek közötti VPN-funkciókkal a vállalatok az alacsony költségű internetes kapcsolatok révén biztonságosan kiterjeszthetik hálózataikat üzleti partnereikig, illetve a távoli helyszínekre és nemzetközi kirendeltségekre. Az 5. táblázat a hálózathoz alkalmazkodó, telephelyek közötti VPN jellemzőit ismerteti.

**5. táblázat** Telephelyek közötti VPN-kapcsolat

| Jellemzők | Leírás |
|---|---|
| **QoS-re alkalmas** | Ügyel a késleltetésérzékeny alkalmazásokra, így a hang- és videoátvitelre, valamint a terminálszolgáltatásokra. |
| **Hálózathoz alkalmazkodó útvonalválasztás** | Az Open Shortest Path First (OSPF) útválasztó szolgáltatások támogatják a szomszédos csomópontok csatornákon keresztüli kapcsolatát, és ezzel elősegítik a hálózatok közötti együttműködést megkönnyítő hálózati topológiafigyelést. |

## A VPN-EK HATÉKONYABBÁ TÉTELE

A Cisco ASA 5500 sorozat számos funkciót, így például biztonsági és terheléselosztási lehetőségeket foglal magában, amelyek lecsökkentik a VPN méretezéséhez és biztonságossá tételéhez szükséges készülékek számát. Ezzel pedig a berendezések költsége, az architektúra összetettsége, valamint az üzemeltetési költségek is csökkenthetők.

**6. táblázat** A VPN-t kiegészítő integrált funkciók

| Jellemzők | Leírás |
|---|---|
| **Hálózati és végpontbiztonság** | A rosszindulatú programok hardveres elhárítása, IPS-sel és tűzfalfunkciókkal megnövelt VPN-biztonság a telepítendő eszközök számának csökkentése mellett |
| **Terheléskiegyenlítés** | A beépített terheléskiegyenlítési funkciók többkészülékes clusterek létesítését teszik lehetővé, feleslegessé téve a költséges külső terheléskiegyenlítő eszközöket |

## A CISCO ASA 5500 PLATFORM ÁTTEKINTÉSE

A Cisco ASA 5500 sorozat öt modellje (az 5505, 5510, 5520, 5540 és 5550) a kis irodáktól kezdve egészen a nagyvállalati központokig tökéletesen lefedi a különböző igényeket (3. ábra). Valamennyi modell azonos házzal készül, és kiválóan alkalmas párhuzamos szolgáltatásbővítésre, megfelelő védelmet biztosít az eddigi beruházásokhoz, és tökéletesen bővíthető a későbbi technológiákkal. A 7. táblázat a Cisco ASA 5500 sorozat különböző modelljeinek specifikációját tartalmazza.

**3. ábra** A Cisco ASA 5500 sorozat

**7. táblázat** A Cisco ASA 5500 sorozatú adaptív biztonsági berendezések specifikációja

| | Cisco ASA 5505 | Cisco ASA 5510 | Cisco ASA 5520 | Cisco ASA 5540 | Cisco ASA 5550 |
|---|---|---|---|---|---|
| **Max. átviteli sebesség** | 100 Mbit/s | 170 Mbit/s | 225 Mbit/s | 325 Mbit/s | 425 Mbit/s |
| **Maximális egyidejű IPsec-kapcsolatok száma** | 25 | 250 | 750 | 5000 | 5000 |
| **Maximális egyidejű SSL alapú VPN-kapcsolatok száma** | 25 | 250 | 750 | 2500 | 5000 |
| **Csatlakozók** | Nyolc 10/100 megabites rézvezetős Ethernet-port dinamikus port–csoportosítással (közülük kettő Ethernet-kábeles tápellátást is biztosít), három USB-port | Három 10/100/1000 megabites rézvezetős Ethernet-port, egy sávon kívüli felügyeletű port, két USB-port | Négy 10/100/1000 megabites rézvezetős Ethernet-port, egy sávon kívüli felügyeletű port, két USB-port | Négy 10/100/1000 megabites rézvezetős Ethernet-port, egy sávon kívüli felügyeletű port, két USB-port | Nyolc Gigabit Ethernet port, négy üvegszálas SFP-port, egy Fast Ethernet port |
| **Profil** | Asztali készülék | 1 U | 1 U | 1 U | 1 U |
| **Stateful failover** | Nincs | Külön licenszet igénylő funkció* | Igen | Igen | Igen |
| **VPN-terheléselosztás** | Nem | Licenszelt szolgáltatás* | Igen | Igen | Igen |

* Licenszbővítés a Cisco ASA 5510 Security Plus licenszcel együtt kapható

## 8. táblázat Rendelési adatok – Készülék és licenszek egy csomagban

A 8. és 9. táblázat a Cisco ASA 5500 sorozatú SSL/IPsec VPN Edition készülékek rendelési adatait tartalmazza. A Cisco ASA 5500 sorozat valamennyi készüléke alapkiépítésben biztosítja a maximális számú egyidejű IPsec-felhasználó kiszolgálását. Valamennyi SSL VPN-funkció elérhető egyetlen funkciólicensszel. A termékcsalád tagjai az SSL VPN-licensz megvásárlása után támogatják az SSL VPN-szabványt. Ez közös cikkszámmal a termékkiadással együtt, egy csomagban is megvásárolható, de a készülék és az SSL VPN-funkciólicensz külön-külön is beszerezhető (lásd a 8. táblázatot). Rendelés leadásához látogasson el a Cisco rendelési honlapjára.

| SSL VPN felhasználói követelmények | A termékkel egy csomagban vásárolható | Csomag cikkszáma |
|---|---|---|
| **10 SSL VPN-felhasználó** | Cisco ASA 5505 SSL / IPsec VPN Edition 10 egyidejű SSL VPN-felhasználónak | ASA5505-SSL10-K9 |
| **25 SSL VPN-felhasználó** | Cisco ASA 5505 SSL / IPsec VPN Edition 25 egyidejű SSL VPN-felhasználónak | ASA5505-SSL25-K9 |
| **50 SSL VPN-felhasználó** | Cisco ASA 5510 SSL / IPsec VPN Edition 50 egyidejű SSL VPN-felhasználónak | ASA5510-SSL50-K9 |
| **100 SSL VPN-felhasználó** | Cisco ASA 5510 SSL / IPsec VPN Edition 100 egyidejű SSL VPN-felhasználónak | ASA5510-SSL100-K9 |
| **250 SSL VPN-felhasználó** | Cisco ASA 5510 SSL / IPsec VPN Edition 250 egyidejű SSL VPN-felhasználónak | ASA5510-SSL250-K9 |
| **500 SSL VPN-felhasználó** | Cisco ASA 5520 SSL / IPsec VPN Edition 500 egyidejű SSL VPN-felhasználónak | ASA5520-SSL500-K9 |
| **1000 SSL VPN-felhasználó** | Cisco ASA 5540 SSL / IPsec VPN Edition 1000 egyidejű SSL VPN-felhasználónak | ASA5540-SSL1000-K9 |
| **2500 SSL VPN-felhasználó** | Cisco ASA 5540 SSL / IPsec VPN Edition 2500 egyidejű SSL VPN-felhasználónak | ASA5540-SSL2500-K9 |
| **2500 SSL VPN-felhasználó** | Cisco ASA 5550 SSL / IPsec VPN Edition 2500 egyidejű SSL VPN-felhasználónak | ASA5550-SSL2500-K9 |
| **5000 SSL VPN-felhasználó** | Cisco ASA 5550 SSL / IPsec VPN Edition 5000 egyidejű SSL VPN-felhasználónak | ASA5550-SSL5000-K9 |

## 9. táblázat Adatok egyedi cikkek külön rendeléséhez

| Válassza ki a Cisco ASA készülékházat és az SSL VPN-licenszfokozatot | | | | | | |
|---|---|---|---|---|---|---|
| SSL VPN – felhasz-nálói követelmények | Cikkszám | Cisco ASA 5505 | Cisco ASA 5510 | Cisco ASA 5520 | Cisco ASA 5540 | Cisco ASA 5550 |
| 10 SSL VPN-felhasználó | ASA5500-SSL-10 | X | X | X | X | X |
| 25 SSL VPN-felhasználó | ASA5500-SSL-25 | X | X | X | X | X |
| 50 SSL VPN-felhasználó | ASA5500-SSL-50 | – | X | X | X | X |
| 100 SSL VPN-felhasználó | ASA5500-SSL-100 | – | X | X | X | X |
| 250 SSL VPN-felhasználó | ASA5500-SSL-250 | – | X | X | X | X |
| 500 SSL VPN-felhasználó | ASA5500-SSL-500 | – | – | X | X | X |
| 750 SSL VPN-felhasználó | ASA5500-SSL-750 | – | – | X | X | X |
| 1000 SSL VPN-felhasználó | ASA5500-SSL-1000 | – | – | – | X | X |
| 2500 SSL VPN-felhasználó | ASA5500-SSL-2500 | – | – | – | X | X |
| 5000 SSL VPN-felhasználó | ASA5500-SSL-5000 | – | – | – | – | X |

## CISCO-SZOLGÁLTATÁSOK

A Cisco Systems szolgáltatásai keretében nyújt segítséget a biztonsági megoldások telepítéséhez és felügyeletéhez. A Cisco teljes élettartamra vonatkozó megközelítési módot alkalmaz a szolgáltatások körében, amely a Cisco adaptív biztonsági készülékek, illetve a Cisco egyéb biztonsági technológiáinak telepítésére és üzemeltetésére vonatkozó követelményeket adja meg. Ezáltal fejleszthető a hálózat átfogó biztonsági szintje, melynek nyomán nagyobb rendelkezésre állású és megbízhatóbb hálózat építhető ki, fel lehet készülni az új alkalmazások bevezetésére, csökkenthetők a hálózati költségek, és napi szinten biztosítható a hálózat egészséges működése. További tájékoztatás a Cisco biztonsági szolgáltatásairól: http://www.cisco.com/go/services/security.

## TOVÁBBI INFORMÁCIÓK

További információkért kattintson az alábbi hivatkozásokra:

Cisco ASA 5500 sorozat:

http://www.cisco.com/go/asa

Cisco Adaptive Security Device Manager:

http://www.cisco.com/go/asdm

Cisco termékminősítés:

http://www.cisco.com/go/securitvcert

A Cisco technikai támogatása:

http://www.cisco.com/en/US/products/svcs/ps3034/serv category home.html

Cisco Advanced Services:

http://www.cisco.com/go/services

Cisco behatolásmegelőző rendszerek:

http://www.cisco.com/en/US/products/ps6076/serv group home.html