

McAfee Firewall Enterprise Alkalmazás

Teljes körű jellemzést ad, és tartalmaz minden új fenyegetést és sebezhetőséget

A burjánzó vállalati alkalmazások és a Web 2.0 széles körű, gyorsan változó támadási felületei a tűzfalbiztonság új megközelítését teszik szükségessé. Az első generációs tűzfalak korlátozva voltak portra, protokollra és az IP-címekre. Manapság, a fejlett új generációs McAfee® tűzfalakkal magabiztosan felfedezheti, irányíthatja, láthatóvá teheti és megvédheti az új és meglévő alkalmazásokat, a hatékony, érvényben lévő szabályokhoz alkalmazott vizuális elemzések és a felhasználói azonosítás használatával. Az alkalmazásokon belüli összetett fenyegetések észleléséhez összekötjük a megelőző fenyegetés-hírszerzést többféle vizsgálati technológiával egyetlen költséghatékony, könnyen kezelhető eszközben.

A McAfee Firewall Enterprise eszköz biztonsági funkciói

AppPrism—Alkalmazáskeresés és -irányítás, többek között:

- Adatcsomag, állapotorientált és teljes alkalmazásszűrés
- Teljes alkalmazáskeresés és -irányítás
- Többszörös kézbesítési opciók, többek között több tűzfalas eszközök (egy eszköz akár 32 virtuális tűzfalat is kezel), McAfee Firewall Enterprise for Riverbed alkalmazás és egy virtuális tűzfal
- Hálózaticím-fordítás (Network address translation - NAT)

McAfee AppPrism™ kategóriák

- Névtelenítők / proxik
- Hitelesítési szolgáltatások
- Üzleti web-alkalmazások
- Tartalomkezelés
- Üzleti figyelés
- Adatbázis
- Könyvtárszolgáltatások
- E-mail
- Titkosított csatornák
- ERP/CRM (Vállalatiirányítási programok/Ügyfélkapcsolat-menedzsment)
- Fájlmegeosztás
- Játék
- Azonnali üzenetküldés
- Infrastruktúra-szolgáltatások
- IT-alkalmazások
- Mobil szoftver
- Peer to peer (P2P)
- Fénykép- és videomegeosztás
- Távoli adminisztráció
- Távoli asztal / Terminálszolgáltatások
- Közösségi hálózatok
- Szoftver- / Rendszerfrissítések
- Tárolás
- Streaming média
- Eszközszávok és PC-alkalmazások
- VOIP
- VPN
- Webmail
- Webböngészés
- Webkonferencia

A tűzfalak hagyományosan annyira erősek vagy gyengék, amennyire a felhasználó által meghatározott házirendek. Napjaink összetett Web 2.0 forgalmának hatékony biztonsági házirendjei azonban a dolgok kifinomult megértésén alapulnak, amit nem könnyű elsajátítani. Gyors felfogóképességre van szükség, amely messze túlmegegy a portokon és a protokollokon, és kiterjed a különböző webes alkalmazásokra és felhasználókra, valamint az őket megcélzó kifinomult fenyegetésekre.

Míg a múltban megvárhattuk az aláírásokat, a fenyegetések szédületes tempójú fejlődése ma már a kockázatok megelőző, előrelátó diagnózisát követeli meg. Többféle attribútumot, például a forrás hírnevét, a tartalmat és a viselkedést kell értékelni ahhoz, hogy még az új fenyegetés megerősítése előtt fel lehessen ismerni az ártó szándékot.

Nem elég előre jelezni a fenyegetést. A pontos, időben történő blokkolás koncentrált tevékenységet igényel, amely keresztülmegegy a hagyományos terméksilókon.

Ezek az igények, kiegészülve az előírások teljesítésének igazolására vonatkozó követelménnyel, növelik a hálózati csoport működési feladatait. A költségvetések ennek ellenére továbbra is szűkek. Valamin változtatni kell.

Az elmúlt 15 év legnagyobb újítása a tűzfalak területén

A McAfee Firewall Enterprise 8-as verziójával a McAfee ismét megtalálja a tűzfalat. Három újítás példa nélküli védelmet nyújt hallatlan áron. Az alkalmazás teljes láthatóságát és irányítását, a fenyegetések felderítését a hírnév tudatosítása mellett és a többvektoros támadás elleni védelmet kombinálva javítjuk a hálózat biztonságát, ugyanakkor csökkentjük a munkai igényt és a költségeket.

A tűzfalmegoldás a McAfee Firewall Enterprise termékcsalád alábbi tagjait tartalmazza: McAfee Firewall Enterprise Profiler, McAfee Firewall Enterprise Control Center és McAfee Firewall Reporter.

Napjainkban a hálózati biztonság leggyengébb láncszeme az alkalmazások rétege. Vettük ezért a több különlegesen érzékeny környezet által is megbízhatónak tartott tűzfalat, és hozzáadtunk széles körű alkalmazáskeresést és -irányítást. Ennek köszönhetően most már Ön is meg tudja védeni az új és meglévő Web 2.0 alkalmazásokat az adatszivárgás, a hálózattal való visszaélés és a támadások kockázatával szemben. A McAfee technológiával biztosíthatja, hogy a hálózatát használó alkalmazások hasznat húznak vállalkozásából.

Keresés

A McAfee AppPrism technológia az innovatív Firewall Profiler eszközt használja a teljes adatforgalom azonosításához és a valóban használt alkalmazások felismeréséhez, olyan hasznos összefüggésekkel, mint a forrás, sávszélesség és cél. A titkosított alkalmazásszintű forgalom vizsgálatával kiküszöbölhetők a számítógépes bűnözők és támadók által kedvelt biztonsági rések.

Irányítás

A kifinomult irányítás lehetővé teszi az üzleti szükségleteknek megfelelő házirend átfogó érvényesítését. A házirendek kizárólag IP-címhez, porthoz vagy protokollhoz való igazítása helyett most már készíthet felhasználónevet szerepkörrel és alkalmazásgyűjteménnyel.

A McAfee Firewall Enterprise biztonsági jellemzői (folytatás)**Hitelesítés**

- Helyi
- Microsoft Active Directory
- Az Active Directory átlátható azonosítása (McAfee Logon Collector)
- LDAP (Sun, Open LDAP, Custom LDAP)
- RADIUS
- Microsoft Windows tartományhitelesítés
- Microsoft Windows NTLM hitelesítés
- Útlevél (egyszeri belépés - SSO)
- Erős hitelesítés (SecurID)

Jó rendelkezésre állás (HA)

- Aktív/aktív
- Aktív/passzív
- Kifinomult munkamenet-feladatátvitel
- Távoli IP-figyelés

Global Threat Intelligence

- McAfee TrustedSource™ globális hírvétséggyűjtés
- Geo-location filtering (Földrajzi hely szűrése)
- McAfee Labs

Titkosított alkalmazásszűrés

- SSH
- SFTP
- SCP
- Kétfázisú HTTPS visszafejtés és újratitkosítás

Behatolásmegelőzési rendszer (Intrusion prevention system - IPS)

- Több mint 10 000 aláírás
- Automatikus aláírás-frissítés
- Egyedi aláírások
- Előre beállított aláíráscsoportok

Vírusvédelem és kémprogram-védelem

- Megvéd a kémprogramok, trójaiak és a férgek ellen
- Heurisztikus
- Automatikus aláírás-frissítés

Webszűrés

- Integrált McAfee SmartFilter® szűrés és kezelés
- Java, Active-X, JavaScript, SOAP blokkolása

Antispam

- McAfee TrustedSource globális hírvétséggyűjtés

VPN

- IKEv1 és IKEv2
- DES, 3DES, AES-128 és AES-256 titkosítás
- SHA-1 és MD5 hitelesítés
- 1, 2 és 5 Diffie-Hellmann csoportok
- Házirendben korlátozott csatornák
- NAT-T
- Xauth

Készítsen olyan alkalmazáshasználati szabályokat, amelyek kombinálják az alábbi attribútumokat:

- Üzleti vagy kikapcsolódási cél
- Felhasználóazonosság
- Beágyazott alkalmazás irányítása
- Engedélyezett címek listája (Fehér lista)
- Geo-location

Felhasználóazonosság

Anélkül, hogy betekintésünk lenne és irányíthatnánk a felhasználókat és használatuk környezetét, a tűzfalak nem tudnak védelmet nyújtani az egyre inkább port-ágilis, kiterő és célzott alkalmazásokkal szemben. A McAfee Firewall Enterprise felhasználó tudatos szabályokat és vezérlést alkalmaz az alkalmazások felett.

Amikor egy felhasználó csatlakozik, a rendszer valós időben érvényesíti a jogosultságokat az Ön meglévő felhasználói könyvtárból. A tűzfal gyorsan alkalmazza a felhasználóazonosítóhoz rendelt házirendeket, ami szavatolja az alkalmazás kifejezett használatát.

A felhasználóhoz történő nyomon követéssel a szabályok elég finomak a modern üzleti műveletekhez. Az azonosításalapú szabályok megfelelő üzemi érzéket teremtenek. Egyre több vállalat hagyatkozik nagymértékben a hozzáférésvezérlést támogató felhasználói könyvtárak és az azonosításkezelés egyesített használatára. A felhasználói változások egyszer megtörténnek, majd elterjednek. A biztonsági házirendek naprakészek maradnak a felhasználói közösség változása mellett.

Beágyazott alkalmazásirányítás

A beágyazott alkalmazásirányítás lehetővé teszi az alkalmazáson belüli jogok testreszabását. Például engedélyezheti a Yahoo-t, de blokkolhatja a Yahoo IM-et, vagy engedélyezheti az IM-et bizonyos felhasználói csoportok, például az ügyfélszolgálat vagy az értékesítés, vagy egyes helyek, például a központi iroda számára.

Emellett támogathatja a megfelelő vállalati használatot és a kizárási házirendeket, ha megadja, hogy egy adott alkalmazást mikor lehet és mikor nem lehet használni. A szabályok engedélyezhetik a MySpace használatát ebédidőben például az ügyfélszolgálati csoport számára, míg a pénzügyi alkalmazások nem érhetők el bárki által a VPN-hálózaton keresztül hétvégén.

Sokan próbálnak hasznot húzni a közösségi hálózatok helyeinek biztonsági hiányosságaiból azáltal, hogy elrejtik rakománykódjukat a divatos kisalkalmazásokban. A McAfee szoftverrel engedélyezheti az olyan oldalak jóindulatú elemeihez való hozzáférést, mint a Facebook, mégis minimalizálva az oldalakon belüli veszélyes alkalmazások kockázatát.

Engedélyezett címek listája (Fehér lista)

A fejlett irányítás része, hogy az engedélyezett címek listája lehetővé teszi kizárólag azon alkalmazások forgalmát, amelyeket szükségként vagy megfelelőként hagytak jóvá. A hosszadalmas fekete listákhoz képest az engedélyezett címek listájával csökkenthető a megírandó és fenntartandó szabályok száma.

Geo-location

Ahogy a botnetek elszaporodnak a népszerű közösségi hálózati alkalmazásokban, egyre fontosabbá vált azon csaló alkalmazások lezárása, amelyek megpróbálnak kommunikálni bizonyos helyszínekkel. A geo-location lehetővé teszi ezen kapcsolat megszüntetését, ezzel megakadályozva az adatok elszivárgását, és megelőzve, hogy számítógépes rendszerét visszaélésre használják fel.

Ezen kifinomult vezérlés mellett a szabályok kidolgozásának bonyolultsága is csökken. Valójában egy nézetben csak egy házirend van. Egyetlen egyszerű konzol adja meg az összes szabály hatékony kezeléséhez és védelmek hozzáadásához szükséges opciókat. Ez az egységes modell különösen hasznos az idő előrehaladtával és a csoportoknál, mivel kiemeljük a szabályok kölcsönhatását és az átfedéseket is. A potenciális konfliktusokat kiemelő színes mezőkkel elkerülhetők a hibák, és javítható a teljesítmény.

Láthatóság

Ideje átlépni a szabályok kezeléséről a kockázatkezelésre. A McAfee Firewall Enterprise Profiler leegyszerűsíti a hálózati forgalom értékelését, így Ön gyorsan hozzáadhat új alkalmazásokat. Intuitív vizuális elemzésünk segítségével azonnal megmérheti az egyes szabályváltozások hatékonyságát, így Ön a szabályozásokat úgy állíthatja be, hogy azok a lehető leghasznosabbak legyenek.

A gazdag grafikus eszközök valós időben hasonlítják össze az alkalmazási tevékenységeket, a felhasználó azonosítását, a földrajzi elhelyezkedést és a felhasználási szinteket alapul véve. Könnyedén megnézheti, ki milyen alkalmazást használ. Ez az integrált nézet lehetővé teszi, hogy néhány kattintással megoldja azt, amihez korábban több órnyi megfeszített munkára, kísérletezésre és hibaelhárításra volt szükség. Néhány felhasználó számára a legnagyobb előny az, hogy azonnal láthatja, hogy a probléma oka valóban a tűzfal volt-e, és elnavigálhat egészen a probléma gyökeréig.

McAfee SecureOS® operációs rendszer

Funkciók

- McAfee Type Enforcement® technológia
- Operációs rendszer (OS) előre beállított biztonsági előírásai
- OS részekre osztása
- Hálózati halom szétválasztása

McAfee Firewall Enterprise vezérlőközpont

- Windows grafikus felhasználói felület
- Helyi konzol
- Teljes parancssor
- USB katasztrófa-helyreállítás konfiguráció biztonsági mentése és visszaállítása
- Gyors hibaelhárítás és tűzfalszabály hatásának elemzése a McAfee Firewall Enterprise Profiler szoftverrel (külön megvásárolható)

Naplózás, megfigyelés és jelentés

- On-box naplózás
- Ütemezett naplőarchiválás és -exportálás
- Firewall Enterprise napló softwareExtract format (SEF)
- Exportálási formátumok (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP v1, v2c és v3
- Tartalmaz McAfee Firewall Reporter SEM alkalmazást

Hálózat és útválasztás

- Dinamikus útválasztás (RIP v1 és v2, OSPF, BGP és PIM-SM)
- Statikus útvonalak
- 802.1Q VLAN címkézés
- DHCP ügyfél
- Alapértelmezett útvonal-feladatátvétel
- QoS

Biztonságos kiszolgálók

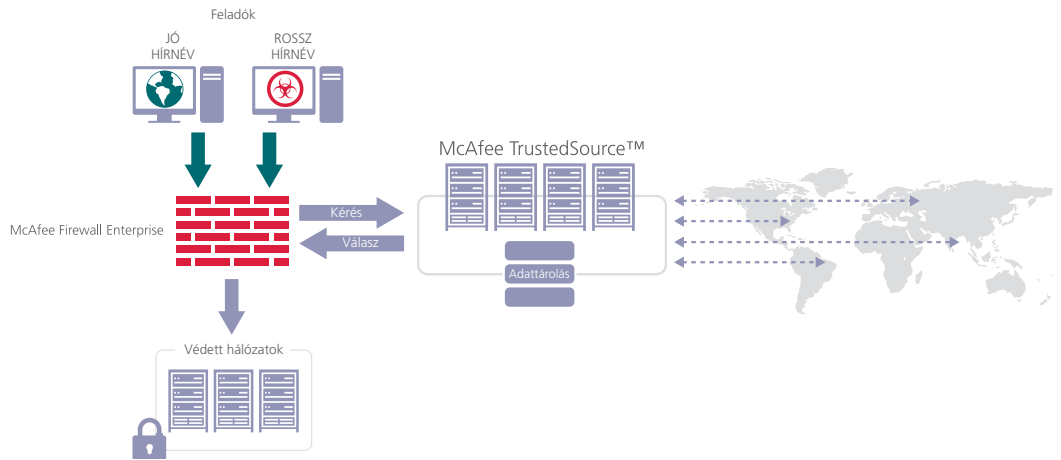
- Biztonságos DNS (egyszeri vagy osztott)
- Biztonságos levélküldés (egyszeri vagy osztott)

Alkalmazások és hardver

- Jótállás átírása négyórás válaszra a legtöbb típusnál
- Elérhető virtualizációs megoldások és robusztus berendezések
- Egy-, két- és négymagos processzorok
- ASIC-alapú gyorsítás
- RAID HDD konfigurációk
- Főlössleges tápellátások

Műszaki támogatás

- A nap 24 órájában elérhető telefonos műszaki támogatás
- A nap 24 órájában elérhető műszaki támogatás weblapú tudásbázissal



A Global Threat Intelligence McAfee Trusted Source szoftvere a hírnév alapján engedélyezi vagy blokkolja a forgalmat

Védelem

A McAfee AppPrism csökkenti az alkalmazásszintű fenyegetések kockázatát, miközben optimalizálja a vállalati sávszélesség használatát. Az AppPrism mögött a McAfee Labs™ teljesítménye munkál. A fenyegetések kutatói a McAfee TrustedSource™ technológiát használják 31 alkalmazáskategória (az anonymizer alkalmazásoktól a video- és fényképmegosztásig) kockázatainak folyamatos felismeréséhez és értékeléséhez.

Ha dinamikus megbízhatóságot rendelünk az oldalakhoz, küldőkhöz és helyszínekhez, blokkolhatjuk a nem kívánt forgalom átlag 70 százalékát, még mielőtt látnánk azt. Ezen képességnek köszönhetően a szoftver megtalálhatja még a botnetek parancs- és irányítási (C & C) csatornáit is.

Ez az egyedüli tűzfal hírnévelemzéssel és global threat intelligence (globális fenyegetések felismerése) technológiával

Egyedül a McAfee tartalmaz hírnév-technológiát a tűzfalban, és ez csak egyik eleme a McAfee Global Threat Intelligence technológiának. A McAfee-nél négyszáznál is több biztonságkutató — több, mint néhány kereskedő alkalmazottainak teljes száma — dolgozik együtt a web, spam, sebezhetőség, hoszt és hálózati behatolások, a kártevők és a szabályozások kérdéseinek kutatásán. Ez a széles kutatási kör lehetővé teszi számukra, hogy minden új fenyegetést és sebezhetőséget jellemezzenek.

Erőfeszítéseik és a százmilliónál is több érzékelőnek a világ minden tájáról érkező információi valós idejű előrejelző kockázatelemzést nyújtanak, hogy megóvják Önt a fejlődő és sokoldalú fenyegetésektől.

Az aláírásokra épülő régi típusú tűzfalakkal ellentétben a McAfee Labstól érkező automatizált fenyegetésadatok naprakészen tartják Önt a tűzfal

hálózati lekapcsolása nélkül. Az olyan fejlett és folyamatos fenyegetések növekedésével, mint az Operation Aurora, a McAfee Global Threat Intelligence technológiája a legkifinomultabb védelmi rendszer, amelyet csak használhat, és amely segít a sebezhetőség csökkentésében, elkerüli a szabályozások megszegését és csökkenti a helyreállítási költségeket.

Többvektoros biztonság egyetlen integrált eszközben

Az egyik ok, amiért az ügyfelek a McAfee-t választják, a kiterjedt biztonsági és megfelelési portfóliónk. Ezt mi most letesszük Ön elé. Szembeszállva a Web 2.0 alkalmazások összetett fenyegetéseivel (rosszindulatú programok, adathalászat és célzott támadások), a McAfee Firewall Enterprise minden tűzfaleszközben ötvözi a kritikus fenyegetésekkel szembeni többszörös védelmet.

Korábban a tűzfalak a hozzáférés-irányításra és szegmentációra voltak korlátozva. A megfelelő védelemhez számos különálló terméket kellett alkalmazni és kezelni. Most egy dobozban megvan minden:

- McAfee AppPrism—Teljes alkalmazáskeresés és irányítás
- Behatolásmegelőzés
- TrustedSource globális hírnévelemzés
- URL szűrés a McAfee SmartFilter® technológiával
- Titkosított alkalmazásszűrés
- Vírusvédelem, kémprogramvédelem és anti-spam

Tapasztalatépítő, többvektoros megoldásaink segítettek nekünk abban, hogy ezeket a védelmi megoldásokat a teljesítmény és a termelékenység kompromisszuma nélkül tudjuk átadni ügyfeleinknek. Mindezt többletdíj nélkül.



McAfee Firewall Enterprise Termékvonal

A Firewall Enterprise termékvonal olyan eszközöket tartalmaz, amelyek megfelelnek az összes vállalatmértéknek, valamint a kísérőtermékeknek, mint amilyen a McAfee Firewall Enterprise Profiler, a McAfee Firewall Enterprise Control Center, és a McAfee Firewall Reporter. Ezek a termékek együttműködnek a kezelési tevékenységek korszerűsítéséért és a működési költségek csökkentéséért. A rugalmas, hibrid szállítási opciók közé tartoznak a fizikai eszközök, a többszörös tűzfaleszközök, a virtuális eszközök és a robusztus használatú környezetek. Kérjen egyedi termékadatlapokat a bővebb információkért.

A kifinomult irányítás kezelhetővé vált

A megbízható biztonságot könnyen is kell tudni konfigurálni. Az intuitív Firewall Enterprise adminisztratív konzol lehetővé teszi a rendszergazdák számára szabályok létrehozását és a védelmek szelektív alkalmazását, például az alkalmazásszűrőket, IPS aláírásokat és az URL szűrést egyetlen képernyőn. Az új szoftverfrissítések automatikusan letöltődnek az internetről, csökkentve a karbantartásra felhasznált időt és energiát. Egyetlen kattintással meg lehet adni az ütemezést.

A Firewall Enterprise termékvonal további eszközöket tartalmaz a kezelés egyszerűsítéséhez: McAfee Firewall Reporter és McAfee Firewall Enterprise Control Center.

A plusz költség nélkül benne lévő Firewall Reporter szoftver az audit adatfolyamait használható információvá alakítja át. Ez a díjnyertes biztonsági eseménykezelő (SEM) eszköz központi megfigyeléssel, viszonyított riasztással és jelentéssel rendelkezik. Válasszon a több mint 500 grafikus jelentés közül a hálózati forgalom ábrázolásához, és minden fontosabb szabályozási követelménynek meg fog felelni.

A külön megvásárolható McAfee Firewall Enterprise Control Center alkalmazás központosított tűzfalházi rend-kezelést nyújt több Firewall Enterprise eszközhöz is. Segítségével maximalizálhatja a működés hatékonyságát, egyszerűsítheti a szabályozás irányítását, optimalizálhatja a szabályokat, korszerűsítheti a szoftverfrissítéseket és igazolhatja a szabályozások betartását. Emellett összevetheti házi rend-konfigurációit az összes kezelőegység által kezelt készüléken, így

biztosítva a hálózat egységességét. A robusztus konfigurációkezelés lehetővé teszi az összes házi rend-módosítás központi követését és érvényesítését.

Továbbá, a kezelőegység integrálódik a McAfee ePolicy Orchestrator® (ePO™) alkalmazással, ezáltal az ePO belátást nyer a tűzfal egészségi állapotának adatai és jelentései közé.

A legbiztonságosabb tűzfalhardver-platform

A McAfee Firewall Enterprise a nagy sebességű, nagyon megbízható McAfee SecureOS operációs rendszeren fut. A szabadalmaztatott McAfee Type Enforcement® technológia biztosítja az operációs rendszert a platformbiztonság páratlan szintjén. Talán éppen ezért rendelkezik a SecureOS páratlan CERT Advisory rekorddal: még soha nem volt szükség vészhelyzeti biztonság javítására.

Az operációs rendszer előre beállított biztonsági előírásai meggátolják a veszélyhelyzeteket, és a teljes operációs rendszer részekre van felosztva, hogy a támadók ne tudják megzavarni munkáját.

Ezekkel az extra lépésekkel ez az első tűzfal, amely megkapta a Common Criteria EAL 4+ igazolást az USA Védelmi Minisztériumának Protection Profile elismerésével együtt.

Újításaink és fejlett biztonságunk miatt a McAfee Firewall Enterprise világszerte 15 000 hálózat védelmét látja el, köztük több ezer kormányhivatal, Fortune 500 szervezet és hét vezető pénzügyi intézmény található. Védje meg magát velünk.



Hardverjellemzők ¹	S1004	410	510	1100	2100	2150	2150 VX-XX	4150
Alaktétyező	Mini 1U	Kis 1U	Kis 1U	Vállalati 1U	Vállalati 2U	Vállalati 2U	Vállalati 2U	Vállalati 5U
Korlátlan felhasználói licenck	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Ajánlott felhasználók	100	300	600	Köz.-Nagy	Köz.-Nagy	Nagy	Nagy	Vállalati
RAID	-	-	-	RAID 1	RAID 1	RAID 5	RAID 5	RAID 5
Tápellátás	Egyszeri	Egyszeri	Egyszeri	Kettős	Kettős	Kettős	Kettős	Kettős
Rézinterfészek (alap/max)	4-Gb	8-Gb	8-Gb	10/16-Gb	10/22-Gb	10/22-Gb	22/24-Gb	14/26-Gb
Szálinterfész opció (max)	-	-	-	6	12	12	-	12
10 Gb interfész opció (max)	-	-	-	6	6	6	6	6
SSL/HTTPS visszafejtés, szűrés és újratitkosítás	Igen	Igen	Igen	Igen	Igen	Igen	Igen	Igen
Betartott szabványok és előírások	FCC (csak USA) Class B, ICES (Kanada) Class B, CE jelölés (EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3), VCC (Japán) Class B, BSMI (Tajvan) Class A, C-Tick (Ausztrália/Új-Zéland) Class B, SABS (Dél-Afrika) Class B, MIC (Korea) Class B, UL 60950, CAN/CSA C22.2 No. 60950, IEC 60950							
Teljesítmény¹								
Tűzfal teljesítménye ²	500 Mbps	1 Gbps	2 Gbps	6 Gbps	6 Gbps	10 Gbps	6 Gbps	12 Gbps
Kifinomult ellenőrzési teljesítmény	300 Mbps	750 Mbps	1,5 Gbps	3 Gbps	3 Gbps	5 Gbps	5 Gbps	6,5 Gbps
Alkalmazásshűzési teljesítmény	100 Mbps	600 Mbps	1,2 Gbps	2,5 Gbps	2,5 Gbps	3,5 Gbps	4 Gbps	5 Gbps
Vírusvédelem	50 Mbps	115 Mbps	275 Mbps	500 Mbps	500 Mbps	850 Mbps	850 Mbps	1 Gbps
IPSec VPN teljesítmény	100 Mbps	200 Mbps	275 Mbps	300 Mbps	300 Mbps	400 Mbps	400 Mbps	700 Mbps
Méret, tömeg, környezet								
Szélesség	27,2 cm	44,7 cm	44,7 cm	48,2 cm	44,3 cm	44,3 cm	44,3 cm	48,25 cm
Mélység	19,5 cm	42,54 cm	54,6 cm	77,2 cm	68,1 cm	68,1 cm	68,1 cm	62,1 cm
Magasság	4,4 cm	4,2 cm	4,2 cm	4,26 cm	8,64 cm	8,64 cm	8,64 cm	21,77 cm
Tömeg	4 kg	6,94 kg	11,8 kg	17,7 kg	26,1 kg	26,1 kg	26,1 kg	35 kg
Tápellátás adatai	45 W 110/220 V	345 W 110/220 V	345 W 110/220 V	Kettős 717 W 110/220 V	Kettős 870 W 110/220 V	Kettős 870 W 110/220 V	Kettős 870 W 110/220 V	Kettős 870 W 110/220 V
Működési hőmérséklet	0 °C – 40 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C	10 °C – 35 °C

1 Minden műszaki jellemző és teljesítményeredmény az S- és F-sorozatú eszközöket veszi alapul.

2 A teljesítményadatok a rendszerek maximális teljesítményét mutatják optimális tesztkörülmények között mérve. A telepítéssel és házirenddel kapcsolatos szempontok hatással lehetnek a teljesítményeredményekre.

