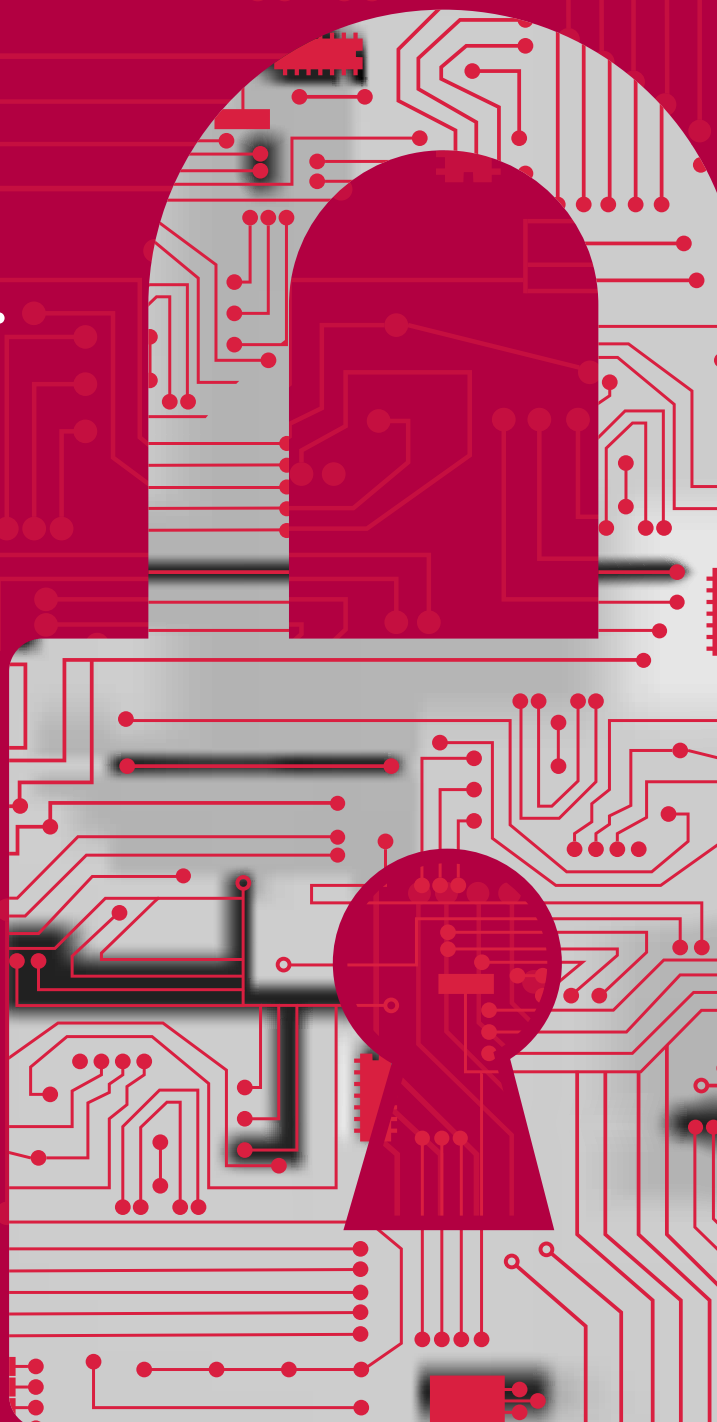


ZYXEL

Mit jelent az ÁAK az SMB protokollal szemben

**Trust Zyxel.
Your Networking Ally.**



GDPR. Cselekedjen!

A zsarolóvírusok és kártevők révén jelentkező internetes támadások fenyegetése nagyon is valós.

Most, hogy a GDPR (általános adatvédelmi rendelet) is érvénybe lépett, még fontosabb, hogy a vállalkozások megfelelő szintű hálózati biztonságot alkalmazzanak, és hogy védjék ügyfeleik adatait.

Számos vállalkozás tévesen hiszi, hogy a GDPR rendelet nem vonatkozik rájuk, mások pedig nem vesznek tudomást a rendeletről, remélve, hogy azt majd eltörlik. Nem ez a helyzet – minden vállalkozásnak be kell tartania az említett rendelet előírásait.

A rendelet az egyes országok adatvédelmi jogszabályait cseréli le, segítve a tisztán látást, és egyetlen jogszabályba dolgozva össze azokat. Ezekkel a módosításokkal megjelent a vállalkozási hálózatok szigorúbb biztonságára vonatkozó követelmény.

Mi az a GDPR?

A GDPR a 95/46/EK sz. adatvédelmi irányelv helyébe lép, és kifejti a minimális követelményeket az EU-állampolgárok személyes adatainak védelme és az EU-n belüli szabad adatáramlás érdekében.

A vállalkozásoknak törvényben előírt kötelezettsége az előírások betartása. A rendelet az Európai Unió minden tagállamára és a Brexit utáni Egyesült Királyságra egyaránt érvényes. Továbbá kiterjeszti a joghatóságot minden olyan vállalatra – függetlenül a vállalat földrajzi elhelyezkedésétől vagy az adatok kezelésének, illetve feldolgozásának helyétől –, amely az EU-ban lakó bármely személyek személyes adatait feldolgozzák.

A rendelet megszegése súlyos pénzbírságot és biztosan további intézkedéseket vonhat maga után a vállalkozás szempontjából, mivel próbára teszi az ügyfelek bizalmát.

Ha úgy találják, hogy egy vállalkozás nem tesz eleget a GDPR-nak, és a vállalkozásnál az adatokat érintő betörés tapasztalható, akkor az akár 20 millió eurós, illetve a teljes éves bevétel akár 4%-ának megfelelő pénzbüntetést kockáztathat - attól függően, melyik a nagyobb.

Ennek kiegészítéseként, amennyiben az adatok sérelme tapasztalható, vagy ha az adatokat nem megfelelően kezelik, a magánszemélyeknek joguk van ahhoz, hogy a rendelet alapján benyújtsák a kártérítési igényüket a kis és nagymértékű megsértése esetén.

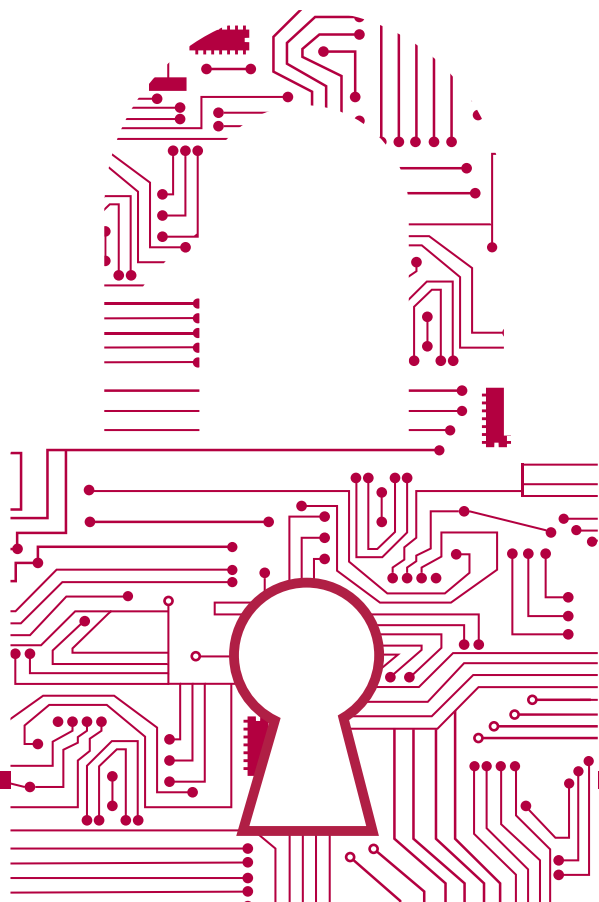
A 32-es cikk kimondottan a vállalkozásokra vonatkozó adatvédelmi követelményekről szól, amely az adatok biztonságos hozzáférését és feldolgozását mondja ki. Miszerint:

[A vállalkozásoknak kell legyen]... egy protokollja arra a rendszeres ellenőrzésre, amely elemzi és kiértékeli a technikai és szervezeti intézkedések hatékonyságát a feldolgozás biztonságosságának tekintetében.

Kötelező jellegű a vállalatok számára, hogy magas szintű hálózati védelemmel rendelkezzenek a GDPR-nak való megfelelés érdekében. A hálózatokat és számítógépeket érő, mind gyakoribb és kifinomultabb internetes támadások miatt létfontosságú, hogy minden vállalkozás komolyan vegye a GDPR-t.

Az előírások betartása szempontjából az első lépés a hálózati biztonság megfelelő szintjének megvalósítása, hogy az adatok titkossága ne sérülhessen.

Auditálás indítása



Az Ön adatainak biztonsága

A vállalkozásoknál a helyükön kell, hogy legyenek azok a rendszerek, amelyek biztosítják az általuk tárolt saját és ügyfeladatok biztonságát. Lehet, hogy ez a múltban alacsonyabb szinten élvezett csak elsőbbséget, de most, hogy a GDPR életbe lépett, és hogy a kiberbűnözők részéről fokozódik a fenyegetés, mára már nincs más választása a vállalkozásoknak, mint hogy komolyan vegyék a hálózati biztonságot.

Az adatokat érintő betöréseket azonnal jelenteni kell az adatvédelmi hatóságnak és az érintett személyeknek, mégpedig 24 órán belül. Akár egy kisebb jogsértés is elég ahhoz, hogy tönkre tegye a vállalkozást, akár a pénzbírság, akár a hírnév elvesztése miatt.

A rendelet előírja, hogy a személyes adatok megfelelő védelmére van szükség azok véletlenszerű vagy jogellenes megsemmisülése, az adatvesztés vagy adatváltoztatás ellen. A nem megfelelő biztonság és a rossz monitorozás nem opció.

Ahhoz, hogy az előírásoknak megfelelhessenek, a vállalkozásoknak több intézkedést is be kell vezetniük, amelyek magukban foglalják a részletes dokumentációt, a regisztrációt és a biztonsági kockázatok felmérését.

A vállalkozásoknak titkosítási és hatékony, valós idejű adatvédelmi intézkedéseket kell bevezetniük, amelyeknek alapfeltétele az innovatív és folyamatosan frissített hálózati védelmi technológiák alkalmazása.

Egyszerű, nagy teljesítményű hálózatvédelem

Míg a technológia számos tekintetben jelentősen egyszerűsítette életünket, a munkavégzés és együttműködés különböző módjai a vállalkozásoknak gyakran kihívásokat jelentenek.

A hálózatokhoz hozzáférő egyre nagyobb számú okoseszköz kezelése, a felhőalapú termelékenységi alkalmazások rangsorolása és blokkolása, valamint a napi webalapú behatolások és támadások elleni védelem soha nem volt fontosabb.

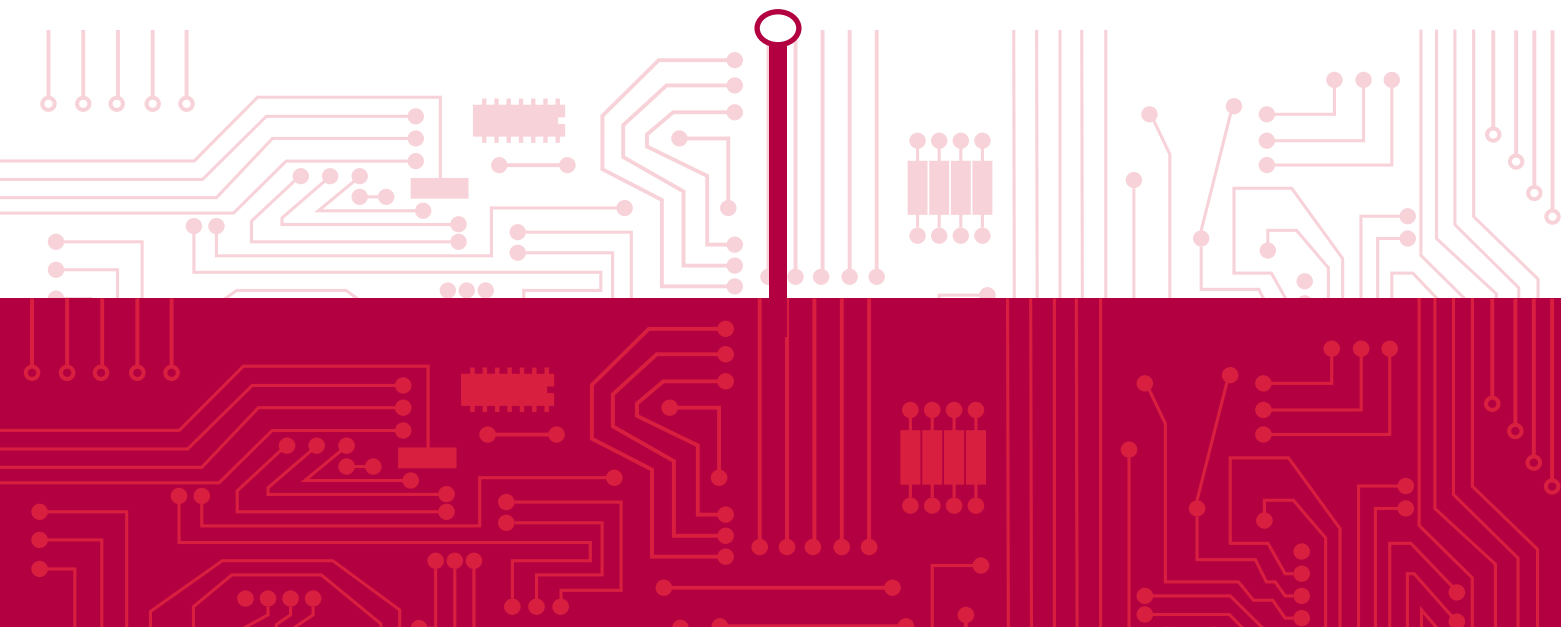
A fenyegetések fejlődésével és a kihívások változatosabbá válásával a vállalkozásoknak is egyre nehezebbé válik az említett kihívásoknak való megfelelés. A közösségi, termelékenységi és más webes alkalmazások szabályozására, optimalizálására és blokkolására alkalmas hatékony megoldás nélkül a vállalkozások a munkatermelékenység csökkenését és azt kockáztatják, hogy vállalkozásuk hálózatai új webes fenyegetéseknek és az adatokat érintő betöréseknek vannak kitéve. A GDPR figyelembevételével ez már nem opció.

Sok kis és közepes vállalkozás nem összpontosított a biztonságra – de most már ideje befektetnie ezen a területen –, és ez nem is kell, hogy költséges vagy bonyolult legyen.

A Zyxel a következő generációs Unified Security Gateway (USG) (egységes biztonsági átjáró) teljes csomagját kínálja, amely áthatolhatatlan védelmet nyújt a rosszindulatú programok és a jogosulatlan alkalmazások ellen. Mindezt a deep packet inspectionnel kombinálva a Zyxel USG-választéka a kézenfekvő megoldás a vállalkozások zsarolóvírusok elleni védelme és a GDPR-feltételeknek való megfelelés biztosítására.

LÉPJEN MOST!

Ne várjon addig, amikor már túl késő!



Zyxel integrált biztonsági megoldások

USG-sorozat

Az USG sorozat teljes mértékben elhárítja az Internetről érkező támadásokat és védelmet nyújt a hackerek ellen. Az anti-spam, anti-vírus, tartalomszűrő, és behatolás érzékelő funkciókat tartalmazó teljes UTM védelem erős megoldást jelent az egyre gyarapodó fenyegetések kezelésére.

- ✓ **UTM** - Teljes hálózati védelem anti-vírus, anti-spam, tartalomszűrés 2.0, IDP és Application Patrol funkciókkal
- ✓ **VPN** - Fiókirodák, partnerek és otthoni felhasználók ZyWALL Tűzfalat telepíthetnek a helyszínről helyszínre való IPsec VPN kapcsolatokhoz
- ✓ **Könnyű használhatóság** - A komplex beállítások kezelése bonyolult és időigényes lehet. A ZyWALL USG-sorozat egy ún. "easy mode" telepítést kínál az új és SOHO felhasználók számára IPsec VPN kapcsolatokhoz



[További információ](#)

ATP-sorozat

A Fejlett Veszélyforrások Elleni Védelem (Advanced Threat Protection - ATP) UTM szolgáltatásokat kínál, de még egy lépéssel tovább megy. A sandboxing technológiát alkalmazva az ATP valós idejű ellenőrzést nyújt az ismeretlen fenyegetések ellen és nulladik napi támadások ellen is védelmet nyújt. Az ATP a megfelelő választás a hálózatok védelmére a hackerek egyre kifinomultabb támadásai ellen.

- ✓ **Sandboxing** - A felhő alapú Sandboxing elszigeteli, lefuttatja és megvizsgálja az ismeretlen programokat, majd analizálja viselkedésüket és megállapítja, hogy ártalmasak vagy nem valós idejűek-e
- ✓ **UTM** - z ATP szervízcsomag olyan klasszikus UTM védelmet tartalmaz, mint a web biztonság és a malware blokkolás
- ✓ **Elemzések** - A SecuReporter elemzi a biztonságot és valós időben egyezteteti az adatokat



[További információ](#)

NSG sorozat

A Zyxel Nebula átjárók gyorsan és könnyen üzembe helyezhetők távoli helyszíneken is a szinte érintés nélküli felhő-konfiguráció segítségével. A rendszer automatikusan konfigurálja a beállításokat, zökkenőmentesen tölti le a firmware és biztonsági aláírás frissítéseket a felhőből, helyszíni hálózatépítési szakértelem szüksége nélkül.

- ✓ **Easy setup** - Providing site-wide visibility and control that enables administrators to manage event logs, traffic statistics, bandwidth consumption, networked clients and application usage without access to individual devices
- ✓ **VPN** - The Security Gateway, either site-to-site or hub-and-spoke VPN connections can be configured with complete simplicity and without complex VPN configuration steps - it's just a few clicks in the Nebula Control Center
- ✓ **Policy Management** - Zyxel Nebula gateways streamline configuration of firewalls and every security feature for faster, easier and more consistent policy settings by supporting object-based management and a unified configuration approach for all security related policies



[További információ](#)

Zyxel integrated Security Defense Technology



Anti-Virus

Prevents the latest content layer threats by detecting and removing malware



Intrusion Detection & Prevention

Checking against network traffic flow to prevent known and unknown stealth cyber threats



Application Intelligence

Allows or denies the use of web applications to prevent threats from entering the network through applications



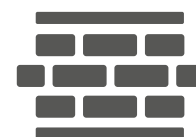
Anti-Spam

Reduce the number of spam messages, control attacks and virus infections via email



WLAN Controller

Integrated in a WLAN control gateway to the radio receiver, reducing the cost of multi-machine deployment



Firewall

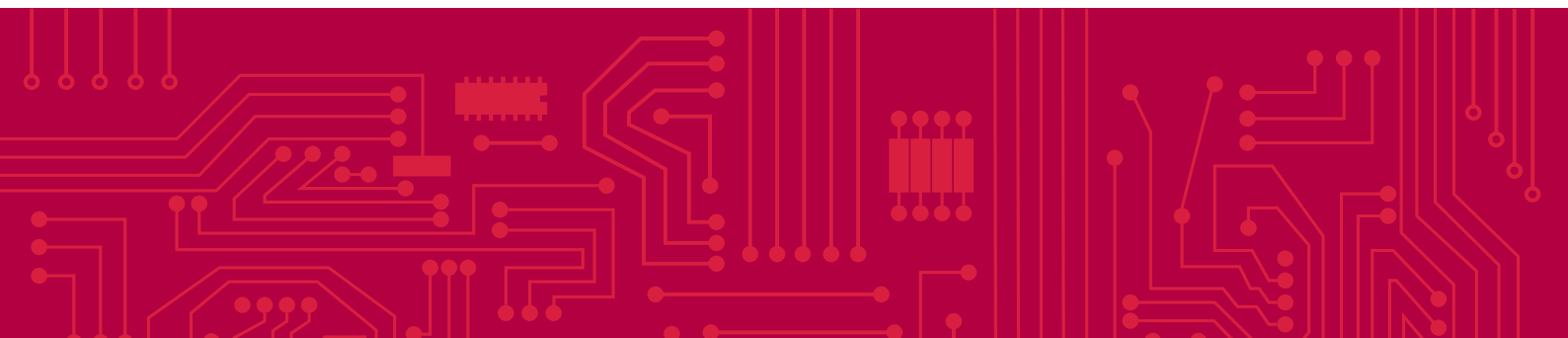
Monitors and controls the incoming and outgoing network traffic

Védje meg a hálózatát!

Nem biztos abban, hogy jelenlegi hálózata biztonságos? Miért nem próbálja ki a biztonsági auditálást? Ez jelezni fogja azt a védelmi szintet, amelyet az Önnél jelenleg alkalmazott megoldás biztosít, és azt is, hol lehet még javítani a dolgokon.

[Kapcsolat](#)

[Auditálás indítása](#)



Corporate Headquarters

Zyxel Communications Corp.

Tel: +886-3-578-3942
Fax: +886-3-578-2439
Email: sales@zyxel.com.tw
http://www.zyxel.com

Europe

Zyxel Belarus

Tel: +375 17 334 6099
Fax: +375 17 334 5899
Email: sales@zyxel.by
http://www.zyxel.by

Zyxel BeNeLux

Tel: +31 23 555 3689
Fax: +31 23 557 8492
Email: sales@zyxel.nl
http://www.zyxel.nl
http://www.zyxel.be

Zyxel Bulgaria (Bulgaria, Macedonia, Albania, Kosovo)

Tel: +3592 4443343
Email: info@cz.zyxel.com
http://www.zyxel.bg

Zyxel Czech Republic

Tel: +420 241 091 350
Hotline: +420 241 774 666
Fax: +420 241 091 359
Email: sales@cz.zyxel.com
http://www.zyxel.cz

Zyxel Denmark A/S

Tel: +45 39 55 07 00
Fax: +45 39 55 07 07
Email: sales@zyxel.dk
http://www.zyxel.dk

Zyxel Finland

Tel: +358 9 4780 8400
Email: myynti@zyxel.fi
http://www.zyxel.fi

Zyxel France

Tel: +33 (0)4 72 52 97 97
Fax: +33 (0)4 72 52 19 20
Email: info@zyxel.fr
http://www.zyxel.fr

Zyxel Germany GmbH

Tel: +49 (0) 2405-6909 0
Fax: +49 (0) 2405-6909 99
Email: sales@zyxel.de
http://www.zyxel.de

Zyxel Hungary & SEE

Tel: +36 1 848 0690
Email: info@zyxel.hu
http://www.zyxel.hu

Zyxel Iberia

Tel: +34 911 792 100
Email: ventas@zyxel.es
http://www.zyxel.es

Zyxel Italy

Tel: +39 011 2308000
Email: info@zyxel.it
http://www.zyxel.it

Zyxel Norway

Tel: +47 22 80 61 80
Fax: +47 22 80 61 81
Email: salg@zyxel.no
http://www.zyxel.no

Zyxel Poland

Tel: +48 223 338 250
Hotline: +48 226 521 626
Fax: +48 223 338 251
Email: info@pl.zyxel.com
http://www.zyxel.pl

Zyxel Romania

Tel: +40 31 0809 888
Fax: +40 31 0809 890
Email: info@cz.zyxel.com
http://www.zyxel.ro

Zyxel Russia

Tel: +7 (495) 539-9935
Fax: +7 (495) 542-8925
Email: info@zyxel.ru
http://www.zyxel.ru

Zyxel Slovakia

Tel: +421 220 861 847
Hotline: +421 220 861 848
Fax: +421 243 193 990
Email: info@cz.zyxel.com
http://www.zyxel.sk

Zyxel Sweden A/S

Tel: +46 8 55 77 60 60
Fax: +46 8 55 77 60 61
Email: sales@zyxel.se
http://www.zyxel.se

Zyxel Switzerland

Tel: +41 (0)44 806 51 00
Fax: +41 (0)44 806 52 00
Email: info@zyxel.ch
http://www.zyxel.ch

Zyxel Turkey A.S.

Tel: +90 212 314 18 00
Fax: +90 212 220 25 26
Email: bilgi@zyxel.com.tr
http://www.zyxel.com.tr

Zyxel UK Ltd.

Tel: +44 (0) 118 9121 700
Fax: +44 (0) 118 9797 277
Email: sales@zyxel.co.uk
http://www.zyxel.co.uk

Zyxel Ukraine

Tel: +380 44 494 49 31
Fax: +380 44 494 49 32
Email: sales@ua.zyxel.com
http://www.ua.zyxel.com

Asia

Zyxel China (Shanghai) China Headquarters

Tel: +86-021-61199055
Fax: +86-021-52069033
Email: sales@zyxel.cn
http://www.zyxel.cn

Zyxel China (Beijing)

Tel: +86-010-62602249
Email: sales@zyxel.cn
http://www.zyxel.cn

Zyxel China (Tianjin)

Tel: +86-022-87890440
Fax: +86-022-87892304
Email: sales@zyxel.cn
http://www.zyxel.cn

Zyxel India

Tel: +91-11-4760-8800
Fax: +91-11-4052-3393
Email: info@zyxel.in
http://www.zyxel.in

Zyxel Kazakhstan

Tel: +7-727-2590-699
Fax: +7-727-2590-689
Email: info@zyxel.kz
http://www.zyxel.kz

Zyxel Korea Corp.

Tel: +82-2-890-5535
Fax: +82-2-890-5537
Email: sales@zyxel.kr
http://www.zyxel.kr

Zyxel Malaysia

Tel: +603 2282 1111
Fax: +603 2287 2611
Email: sales@zyxel.com.my
http://www.zyxel.com.my

Zyxel Middle East FZE

Tel: +971 4 372 4483
Cell: +971 562146416
Email: sales@zyxel-me.com
http://www.zyxel-me.com

Zyxel Philippine

Email: sales@zyxel.com.ph
http://www.zyxel.com.ph

Zyxel Singapore

Tel: +65 6339 3218
Hotline: +65 6339 1663
Fax: +65 6339 3318
Email: sales@zyxel.com.sg
http://www.zyxel.com.sg

Zyxel Taiwan (Taipei)

Tel: +886-2-2739-9889
Fax: +886-2-2735-3220
Email: sales_tw@zyxel.com.tw
http://www.zyxel.com.tw

Zyxel Thailand

Tel: +66-(0)-2831-5315
Fax: +66-(0)-2831-5395
Email: info@zyxel.co.th
http://www.zyxel.co.th

Zyxel Vietnam

Tel: (+848) 35202910
Fax: (+848) 35202800
Email: sales_vn@zyxel.com.tw
http://www.zyxel.com/vn/vi/

The Americas

Zyxel USA

North America Headquarters

Tel: +1-714-632-0882
Fax: +1-714-632-0858
Email: sales@zyxel.com
http://us.zyxel.com

Zyxel Brazil

Tel: +55 (11) 3373-7470
Fax: +55 (11) 3373-7510
Email: comercial@zyxel.com.br
http://www.zyxel.com/br/pt/

For more product information, visit us on the web at www.zyxel.com