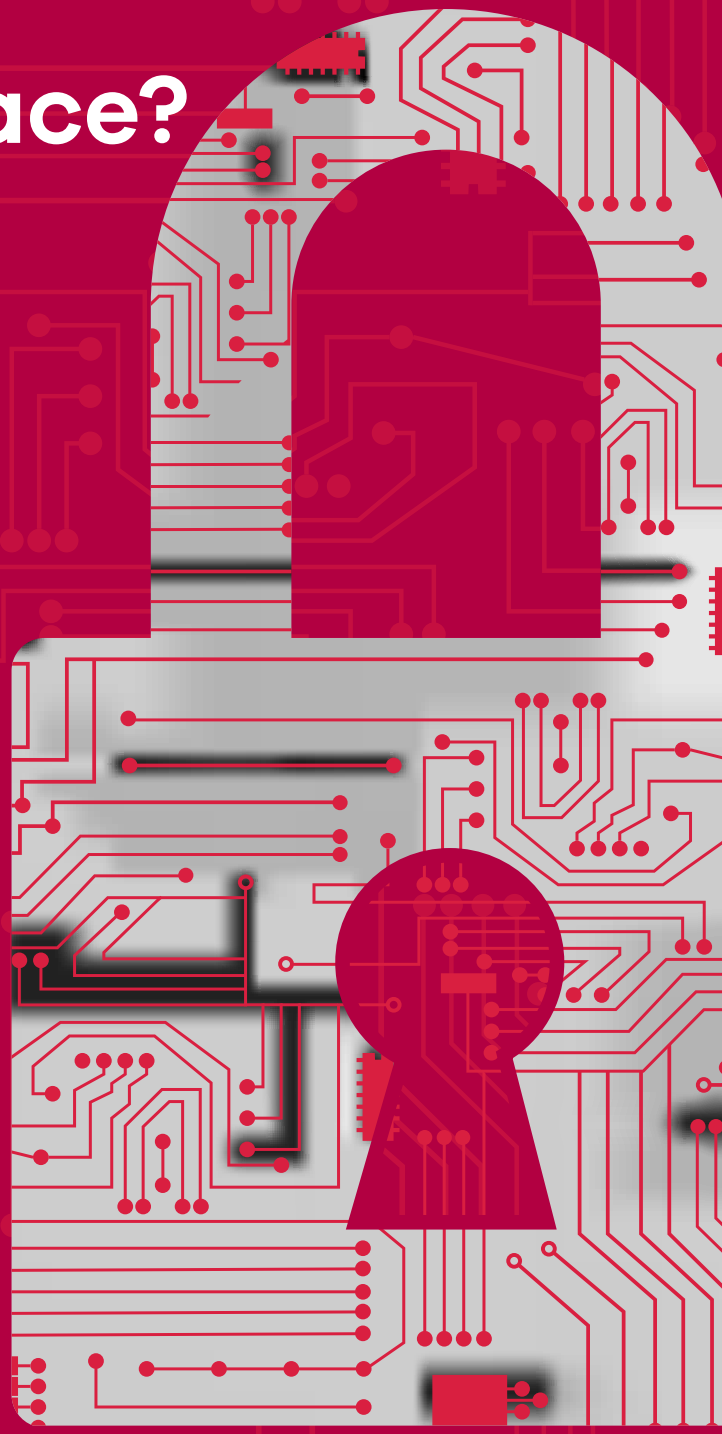


ZYXEL

Co nařízení GDPR znamená pro malé a střední organizace?

Zyxel.

Your Networking Ally.



GDPR. je čas jednat.

Ohrožení firemních sítí kybernetickými útoky v podobě ransomwaru a malwaru je reálné.

Poté, co začalo platit nařízení GDPR (Obecné nařízení o ochraně osobních údajů), je důležitější než kdykoliv v minulosti, aby organizace nasadily správnou úroveň zabezpečení sítí a chránily svá vlastní data i data svých zákazníků.

Mnohé organizace se mylně domnívají, že se jich nařízení GDPR netýká, zatímco jiné ho ignorují a doufají, že nebude mít dlouhou existenci. Skutečnost je však taková, že požadavky tohoto nařízení musí plnit všechny organizace.

Nařízení GDPR nahradilo zákony jednotlivých zemí na ochranu údajů, aby se příslušná legislativa ujasnila a sjednotila do jednoho celku. S těmito změnami přicházejí také vyšší nároky na zabezpečení firemních sítí.

Co je to GDPR?

Nařízení GDPR nahradilo Směrnicí 95/46/ES o ochraně osobních údajů a stanovuje minimální standardy ochrany osobních údajů občanů Evropské unie a volného pohybu údajů v rámci EU.

Společnosti jsou ze zákona povinny toto nařízení dodržovat. Nařízení platí v každé členské zemi Evropské unie včetně Velké Británie po brexitu. GDPR se dále vztahuje na všechny společnosti, které zpracovávají osobní údaje osob žijících v EU bez ohledu na místo, ze kterého tyto společnosti podnikají nebo kde jsou osobní údaje používány či zpracovávány.

Porušení tohoto nařízení může vést k uložení vysokých finančních pokut a k širším dopadům v podobě ztracené důvěry v očích klientů a zákazníků.

Organizacím, které nedodrží nařízení GDPR a u nichž dojde k porušení zabezpečení osobních údajů, mohou být vyměřeny pokuty ve výši až 20 milionů € nebo 4% jejich celkového ročního obrátu podle toho, která hodnota je vyšší.

Bez ohledu na míru jejich závažnosti navíc mají jednotlivci právo požadovat odškodnění za případy porušení zabezpečení osobních údajů nebo za nesprávné zacházení s nimi.

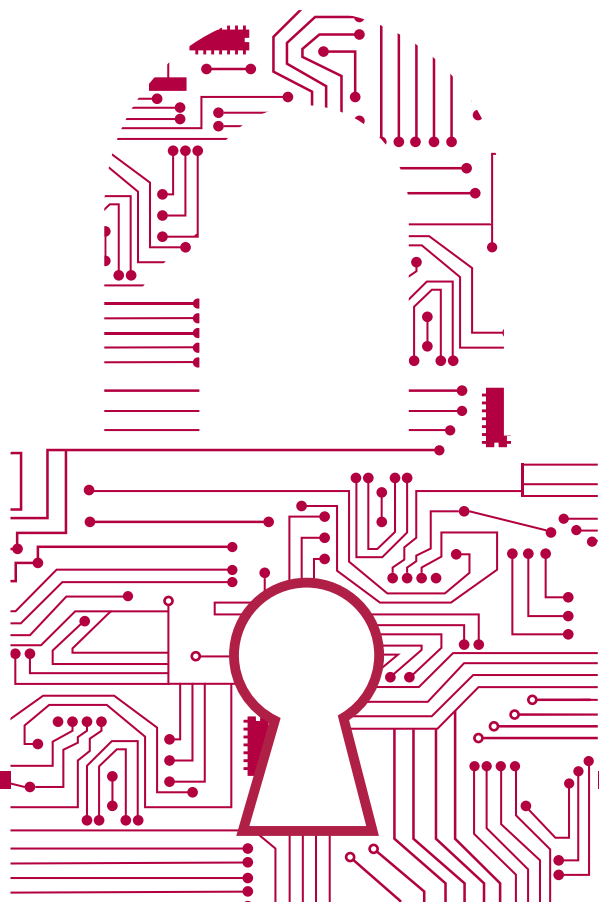
Článek 32 výslovně vyžaduje, aby organizace zavedly robustní zabezpečení údajů, které umožňuje bezpečný přístup k údajům a jejich bezpečné zpracování. V tomto článku se uvádí:

Organizace musí mít ...proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Dodržování požadavků nařízení GDPR od organizací vyžaduje zavedení vysokého standardu síťové bezpečnosti. Vzhledem ke stále častějším a sofistikovanějším kybernetickým útokům na sítě a počítače po celém světě je důležité, aby všechny organizace braly nařízení GDPR vážně.

Pokud chcete zjistit, jestli je vaše síť v současnosti chráněna, vyzkoušejte náš bezplatný bezpečnostní audit.

Absolvujte bezpečnostní audit



Zabezpečení vašich dat

Organizace musí mít zavedeny systémy pro zabezpečení svých vlastních dat i uložených osobních údajů jejich zákazníků. Ačkoliv této problematice nebyla v minulosti vždy věnována dostatečná pozornost, vzhledem k zavedení nařízení GDPR a stále častějším hrozbám kybernetických zločinců je nutné zabezpečení sítí brát vážně.

Případy porušení zabezpečení osobních údajů musí být orgánům pověřeným jejich ochranou a dotčeným osobám oznámeny během 24 hodin. I méně závažné porušení zabezpečení může mít pro organizace likvidační následky, ať už v důsledku vysokých pokut nebo ztráty dobré pověsti.

Nařízení stanoví, že musí být zavedena přiměřená ochrana před náhodným nebo nezákonným zničením, ztrátou nebo falšováním osobních údajů. Nedostatečné zabezpečení a špatný monitoring už nikomu neprojdou.

Pro dodržování nařízení musí organizace zavést opatření, která zahrnují podrobnou evidenci, registraci a vyhodnocení bezpečnostních rizik.

Organizace musí používat šifrování dat a výkonnou ochranu dat v reálném čase, která bude stát na inovativních a průběžně aktualizovaných technologiích pro zabezpečení sítí.

Jednoduchá a přitom robustní ochrana sítí

Ačkoli technologie nepochybně zjednodušují mnoho stránek našeho života, změny ve způsobu práce mohou pro organizace znamenat závažné problémy na poli zabezpečení dat.

Ještě nikdy nebylo tak důležité řádně spravovat zařízení přistupující do sítě, jejichž počet rychle roste, prioritizovat a blokovat širokou paletu cloudových aplikací, které mají dopad na produktivitu, a zajistit ochranu před každodenními průniky a útoky z internetu.

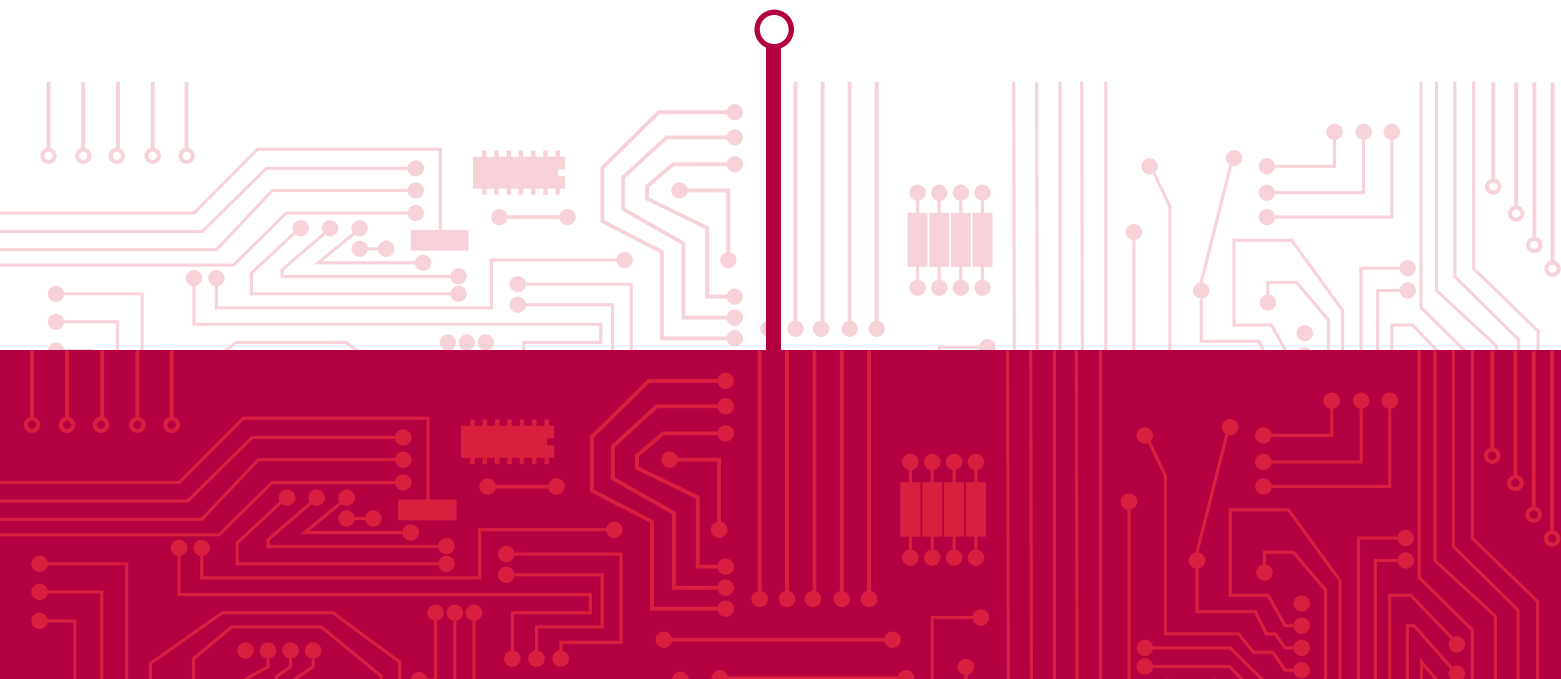
S rostoucí důmyslností a různorodostí hrozeb a výzev je pro organizace stále náročnější udržet věci pod kontrolou. Organizace, které nemají efektivní řešení pro řízení, optimalizaci a potenciální blokování sociálních sítí, aplikací ovlivňujících produktivitu a dalších aplikací, riskují ztrátu produktivity a své sítě vystavují novým hrozbám z internetu a potenciálnímu porušení zabezpečení dat. Něco takového si vzhledem k nařízení GDPR nemůžete dovolit.

Pro mnohé malé a střední firmy zabezpečení sítí doposud bylo okrajovou záležitostí. Nyní ale nastal čas do něj investovat, přičemž to nemusí být ani příliš nákladné, ani příliš složité.

Společnost Zyxel nabízí kompletní portfolio unifikovaných bezpečnostních bran (Unified Security Gateway, USG), které poskytují bezkonkurenční ochranu před malwarem a neoprávněnými aplikacemi. A když se k tomu přidá hloubková kontrola paketů, je řada Zyxel USG jasnou volbou pro organizace, které se chtějí chránit před ransomwarem a plnit požadavky nařízení GDPR.

JEDNEJTE JEŠTĚ DNES.

Nečekejte, až bude příliš pozdě



Integrovaná bezpečnostní řešení Zyxel

Řada USG

Řada USG poskytuje veškerou nezbytnou ochranu před útoky z internetu a hackery. Díky komplexní UTM (jednotná správa hrozeb), která zahrnuje antispam, antivir, filtrování obsahu a detekci průniků, tato řada představuje robustní řešení proti neustále závažnějším nebezpečím.

- ✓ **UTM** - kompletní ochrana sítě pomocí antiviru, antispamu, filtrování obsahu Content Filtering 2.0, detekce a prevence průniků a kontroly aplikací.
- ✓ **VPN** - pobočky, obchodní partneři a domácí uživatelé mohou pomocí firewallů ZyWALL vytvořit site-to-site IPsec VPN připojení.
- ✓ **Ease-of-Use** - správa složitých konfigurací může být nepřehledná a časově náročná. Laikům a uživatelům v malých a domácích kancelářích řada ZyWALL USG poskytuje uživatelské rozhraní s režimem „easy mode“.



[Bližší informace](#)

ATP Series

Naše pokročilá ochrana před hrozbami (ATP) vedle UTM disponuje také technologií sandboxing, která v reálném čase identifikuje neznámé hrozby a chrání před útoky nultého dne. ATP je správnou volbou pro ochranu sítí před stále vynalézavějšími hackery.

- ✓ **Technologie Sandboxing** - slouží ke spouštění a kontrole neznámých programů v izolovaném prostředí, v němž sandbox cloud analyzuje jejich chování a v reálném čase ověřuje, jestli jsou škodlivé.
- ✓ **UTM** - balíček ATP zahrnuje klasickou UTM ochranu, jako např. zabezpečení před hrozbami z internetu a nástroj pro blokování malware.
- ✓ **Analytika** - nástroj SecuReporter analyzuje vaše zabezpečení a provádí korelaci dat v reálném čase.



[Bližší informace](#)

Řada NSG

Díky téměř nulovému nastavování umožňují brány Zyxel Nebula rychlé a snadné nasazení na vzdálených místech. Brána z cloudu automaticky importuje nastavení politik a konfigurace, upgrady firmwaru a aktualizace bezpečnostních podpisů, a její obsluha se tak obejde bez místního síťového odborníka.

- ✓ **Snadné nastavení** - správci mají přehled a kontrolu nad celou sítí, díky čemuž mohou i bez přístupu k jednotlivým zařízením sledovat protokoly událostí a statistiky provozu a řídit využití pásma, klienty v síti i jednotlivé aplikace.
- ✓ **VPN** - bezpečnostní brána umožňuje pomocí několika málo kliknutí v řídicím centru Nebula Control Center velmi jednoduše nakonfigurovat VPN připojení mezi jednotlivými lokalitami (site-to-site) nebo hvězdicově (hub-and-spoke).
- ✓ **Správa politik** - brány Zyxel Nebula podporují správu na bázi objektů a unifikovanou konfiguraci všech bezpečnostních politik. Výsledkem je snadnější konfigurace firewallů a všech bezpečnostních prvků pro rychlejší, jednodušší a kvalitnější nastavení politik.



[Bližší informace](#)

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



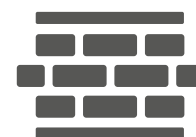
Anti-Spam

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

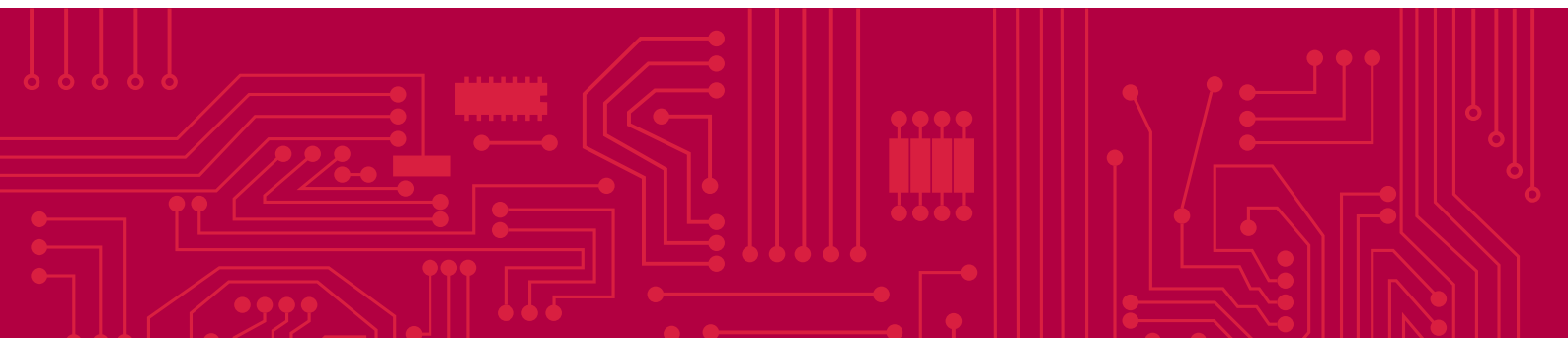
Monitors and controls the incoming and outgoing network traffic

Ochrana vaší sítě

Nejste si jisti, jak dobře je vaše síť zabezpečena? Vyzkoušejte náš bezpečnostní audit! Audit vám ukáže, jakou ochranu vaše současné řešení poskytuje, a také navrhne možná zlepšení.

[Kontaktujte nás](#)

[Spustit audit](#)



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