ZYXEL
NETWORKS

Zabezpečení sítí bez složitostí



Září 2026

Zyxel Networks usnadňuje zabezpečení sítí

Každá malá firma si zaslouží síťové zabezpečení, kterému lze snadno důvěřovat a které je ještě snazší spravovat. To je myšlenka, na níž stojí vše, co Zyxel Networks dělá – a přesně to přinášíme do oblasti kybernetické bezpečnosti.

Svou pověst jsme vybudovali tím, že jsme síťové technologie zpřístupnili malým a středně velkým firmám, přičemž stejný důraz na snadnou dostupnost uplatňujeme také při jejich zabezpečení. Ačkoliv jsme známí především jako společnost vyvíjející síťové přepínače a WiFi zařízení, můžeme se pochlubit také dlouhou historií a bohatými zkušenostmi v oblasti kybernetické bezpečnosti. Tyto zkušenosti se opírají o naši globální bezpečnostní síť a o dlouholeté vztahy s předními dodavateli bezpečnostních řešení.

Tento dokument popisuje, co děláme pro snadné zajištění kybernetické bezpečnosti, proč se náš přístup a nabízená řešení liší od ostatních a čím si získáváme přízeň instalačních firem, integrátorů a poskytovatelů řízených služeb pro malé firmy.



Prostředí hrozeb se mění, a proto jsme vytvořili zabezpečení, které se změnami drží krok

Od raných let internetu, kdy hlavním doporučením bylo zvolit si silné heslo, se kybernetická bezpečnost zásadně proměnila.

Škála hrozeb, kterým firmy musí věnovat pozornost, se za posledních 40 let výrazně rozšířila od pokusů o neoprávněný přístup a škodlivý software až po sofistikované metody, jako např. phishing a ransomware.

Ruku v ruce se stále širší škálou hrozeb se diverzifikovala také ochrana před hrozbami, přičemž z kybernetické bezpečnosti se stalo rozsáhlé specializované odvětví.

Rostoucí složitost zabezpečení sítí je neoddiskutovatelným faktem. Naštěstí firmy nemusí tuto zátěž nést samy.

Kombinovaná ochrana bez složitostí

Věříme, že odpovědí na stále složitější prostředí hrozeb je chytrá konsolidace, nikoliv složitější technologie pro zákazníky.

Tím, že jsme ochranu proti celé škále hrozeb sloučili do jednoho řešení, dokážeme koncovým zákazníkům, včetně těch bez odborných znalostí o kybernetické bezpečnosti, poskytnout zaručenou úroveň ochrany, která výrazně snižuje kybernetická rizika.

Přesně takové řešení nabízí naše firewally řady USG FLEX H, které disponují integrovanou ochranou od předních poskytovatelů profesionálních řešení pro kybernetickou bezpečnost.

Díky kombinaci dashboardu SecuReporter, reportovacích nástrojů a cloudové platformy Nebula pro bezpečnou správu sítí poskytujeme komplexní službu, která malým a středně velkým firmám, živnostníkům i zaměstnancům na home office za dostupnou cenu poskytuje potřebnou kybernetickou ochranu, včetně přehledu o její funkčnosti a možnosti její konfigurace a správy na dálku.

Zpřístupnění kybernetické bezpečnosti firmám

Mnohé malé a středně velké firmy nejenže považují kybernetickou bezpečnost za příliš složitou otázku, ale navíc ani nemají čas zjišťovat, co vlastně potřebují. A malým firmám k tomu ještě mnohdy chybí IT personál nebo odborné znalosti o kybernetické bezpečnosti. Pro mnohé firmy může být problémem už jen nábor a udržení lidí s odpovídajícími zkušenostmi.

V případě firem s omezenými zdroji hrají důležitou roli také náklady na bezpečnostní vybavení a licence.

A právě proto se snažíme, aby naše řešení byla cenově dostupná a snadno obhajitelná. Takže ani nedostatek odborných znalostí nebo omezený rozpočet nemusí znamenat, že firma zůstane bez kybernetické ochrany.



Proč na kybernetické ochraně záleží

Přijetím vhodných preventivních opatření malé firmy výrazně snižují riziko toho, že se stanou obětí kybernetického útoku. Podle průzkumu 2026 SMB Cyber Readiness Index, který provedla společnost ESET, 44 % oslovených organizací v regionu EMEA (Evropa, Blízký východ, Afrika) za posledních 12 měsíců zažilo incident týkající se kybernetické bezpečnosti, zatímco 64 % dotázaných očekává kybernetický útok v příštím roce. Tato čísla dokazují, že kybernetické útoky jsou reálnou hrozbou pro firmy všech velikostí a že příprava na ně se vyplácí.

Úroveň ochrany by měla odpovídat potřebám firmy a míře jejího rizika. Firma, která zpracovává osobní finanční údaje, pravděpodobně disponuje citlivějšími informacemi než například kavárna nebo kadeřnictví. Obecně však platí, že každá firma uchovává data, která stojí za ochranu, od bankovních údajů až po osobní údaje zákazníků a zaměstnanců.

44 % **organizací v regionu EMEA zažilo za posledních 12 měsíců incident týkající se kybernetické bezpečnosti.**



Co všechno musí malé a středně velké firmy chránit

Vhodným místem, kde začít, je ochrana vstupního bodu do sítě, tj. připojení k internetu přes firewall.

Vedle zabezpečení tohoto klíčového bodu je žádoucí, aby všechna připojená zařízení měla nějakou formu ochrany a byla průběžně aktualizována. Vhodnými opatřeními jsou také monitoring a pravidelné kontroly aktivit na síti, zavedení bezpečnostních předpisů a vyškolení zaměstnanců o tom, jak rozpoznat podezřelé emaily a odkazy a jak s nimi nakládat.

Tato opatření nejenže snižují kybernetická rizika, ale také vytvářejí podmínky pro udržení firemních systémů a dat v bezpečí.

I přes přijetí těchto opatření většina firem uvítá spolupráci s partnerem, který za ně převezme každodenní práci spojenou s udržováním licencí a firmwaru v aktuálním stavu a s monitoringem a kontrolou zabezpečení. A právě zde přicházejí ke slovu instalační firmy, integrátoři a poskytovatelé řízených služeb.

Skutečná příležitost pro IT a instalační firmy

Mnohé malé a středně velké firmy se při nastavování notebooků, počítačů a běžných WiFi sítí spoléhají na své vlastní schopnosti nebo na lokální IT odborníky. Pokud jde o kamerové systémy, fyzické zabezpečení, požární hlásiče a chytré technologie, jako např. systémy vstupu do budov, obvykle se pak obracejí na specializované instalační firmy.

Pro lokální IT a instalační firmy představuje kybernetická ochrana skutečnou příležitost získat nový zdroj příjmů.

V minulosti se mnozí tohoto zdroje příjmů raději vzdali kvůli složitosti tehdejších bezpečnostních řešení. Z pochopitelných důvodů nikdo nechce ohrozit cenné vztahy se svými zákazníky. Tuto bariéru nyní překonává náš jednoduchý přístup k zabezpečení.

Díky firewallům řady USG FLEX H dokáží instalační firmy zákazníkům veškerou potřebnou ochranu poskytnout v jednom jediném zařízení. Výchozí nastavení firewallů řady USG FLEX H jsou zvolena tak, aby bez úprav vyhovovala většině malých firem, a celé zprovoznění firewallu usnadňuje pětikrokový proces konfigurace ještě před jeho dodáním.

Snadné nasazení = jasná výhoda

Jednoduché nasazení patří mezi nesporné výhody firewallů značky Zyxel, protože šetří čas, práci i náklady. Zákazníci už nemusí s instalací čekat na návštěvu technika, protože firewall se po připojení do sítě sám nastaví.

Naši obchodní partneři mohou bezpečnostní řešení postavené na firewallech Zyxel nabízet, aniž by byli specialisty na kybernetickou bezpečnost. Zařízení zákazníků mohou na dálku snadno monitorovat a upravovat prostřednictvím naší bezpečné cloudové platformy Nebula.

Okamžitě po instalaci firewall začne poskytovat důkladnou a komplexní ochranu, přičemž kromě udržování bezpečnostní licence a firmwaru v aktuálním stavu vyžaduje jen minimální nebo nulové zásahy.

Pokud už by se náhodou stalo, že provoz firewallu bude vyžadovat naši pomoc, je vždy k dispozici tým odborníků společnosti Zyxel Networks.



Hlavní funkce a výhody firewallů řady USG FLEX H

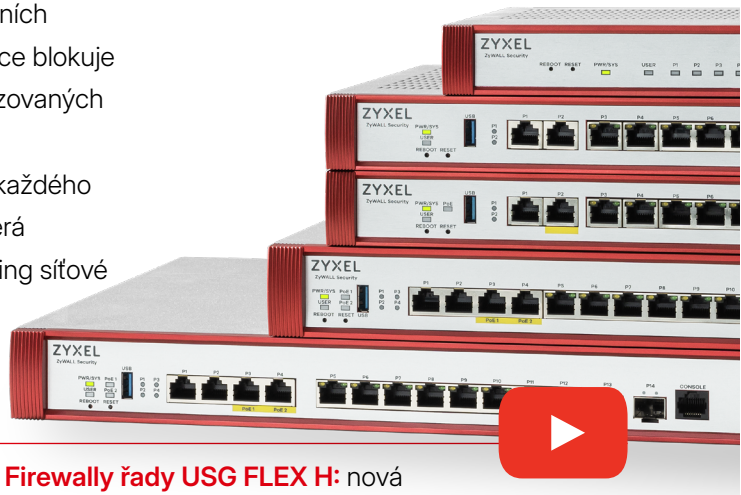
Firewally USG FLEX H od společnosti Zyxel Networks jsou navrženy s důrazem na potřeby a finanční možnosti malých firem. Každý model je standardně vybaven kompletní sadou bezpečnostních funkcí, díky čemuž plnou ochranu nabízí i ten nejmenší a cenově nejdostupnější firewall této řady. Hlavní rozdíl mezi jednotlivými modely spočívá v rychlosti a kapacitě, přičemž vyšší modely jsou určeny pro firmy s více uživateli a větším nároky na propustnost.

Co poskytuje každý firewall řady USG FLEX H

Každý firewall řady USG FLEX H je standardně vybaven následujícími funkcemi:

- **Detekce hrozeb pomocí umělé inteligence:** analyzováním aktuálních globálních dat o hrozbách identifikuje nejnovější a stále sofistikovanější kybernetické útoky a reaguje na ně.
- **Cloudový sandboxing:** v bezpečném prostředí izoluje neznámé nebo podezřelé soubory a před uvolněním analyzuje jejich chování.
- **Systém prevence průniků (IPS):** kontrolou síťového provozu detekuje a blokuje škodlivý payload, snahy o zneužití zranitelností a pokusy o získání neoprávněného přístupu.
- **Filtrování webových stránek a obsahu:** filtruje a blokuje přístup na škodlivé nebo nevhodné webové stránky.
- **Kontrola a řízení aplikací:** identifikuje, klasifikuje a řídí konkrétní aplikace s cílem upřednostnit důležitý provoz a zablokovat používání neschválených aplikací.
- **Kolaborativní detekce a reakce (CDR):** propojuje se s dalšími síťovými zařízeními za účelem provedení automatické karantény nebo zablokování těch zařízení na okraji sítě, která nejsou v pořádku z hlediska bezpečnosti.
- **Robustní podpora VPN:** podpora IPSec VPN pro spojení typu bod-bod i SSL VPN pro vzdálený přístup.
- **Vlastní ochrana a filtrování IP adres dle reputace:** chrání samotný firewall automatickou deaktivací nepoužívaných zranitelných portů. Tato funkce navíc pomocí externích black listů a filtrováním IP adres podle jejich reputace blokuje potenciálně škodlivý provoz přicházející z neautorizovaných zdrojů.
- **Bezpečná cloudová platforma Nebula:** součástí každého firewallu je základní licence k platformě Nebula, která umožňuje vzdálenou správu, konfiguraci a monitoring síťové infrastruktury.

Více informace najdete zde.



Firewally řady USG FLEX H: nová éra kybernetické bezpečnosti.

Dokonalý přehled o zabezpečení

Potenciální zákazníci přirozeně chtějí vědět, co jim vlastně investice do zabezpečení přinese. Dvojnásob to pak platí u firem, které narušení bezpečnosti nebo kybernetický útok doposud samy nezažily.

Dokonalý přehled o účinnosti ochrany poskytované firewally řady USG FLEX H zajišťuje náš cloudový dashboard SecuReporter, který pomocí srozumitelných grafů a diagramů zobrazuje dění v síti, včetně potenciálně škodlivých aktivit. SecuReporter tak představuje snadný a elegantní způsob, jak prokázat přínos kybernetické ochrany.

V dashboardu SecuReporter lze monitorovat nejen veškeré aktivity na síti, ale také soubory preventivně umístěné do cloudového sandboxu a zablokované viry a možné útoky ransomwaru.

A v neposlední řadě SecuReporter poskytuje podrobné informace o chování uživatelů, např. o tom, kdo navštěvuje škodlivé stránky, což firmám pomáhá určit oblasti, na které by se měly více zaměřit jejich bezpečnostní předpisy a školení.



Naše výsledky v oblasti kybernetické bezpečnosti

Jako společnost Zyxel Networks jsme známí zejména díky síťovým přepínačům a WiFi přístupovým bodům. Nicméně již od roku 1999 dodáváme také firewally, přičemž za tu dobu jsme v oblasti kybernetické bezpečnosti získali více než bohaté zkušenosti.

Našim řešením pro ochranu sítí důvěřují stovky tisíc firem po celém světě. Koncoví zákazníci i naši obchodní partneři vědí, že když potřebujete snadné, a přitom nekompromisní bezpečnostní řešení, můžete se vždy spolehnout na společnost Zyxel Networks.

O tom svědčí nespočet ocenění udělených produktům značky Zyxel. Například základní firewall USG FLEX 50HP získal v rámci cen PC Pro Excellence Awards 2025 titul Security Hardware of the Year. Našim firewallům a VPN řešením byl udělen titul Champion v bezpečnostním průzkumu Professional User Ratings (PUR) 2026, který pořádá nezávislá výzkumná společnost *techconsult* a který vychází ze zpětné vazby od tisíců odborníků na kybernetickou bezpečnost.

Vysoký výkon firewallů řady USG FLEX H a účinnost jimi poskytovaného zabezpečení potvrzují mimo jiné nezávislé testy provedené organizací The Tolly Group, která v hodnocení vyzdvihuje zejména vynikající detekci malwaru a celkovou úroveň kybernetické ochrany.

A za zmínku stojí také fakt, že společnost Zyxel Networks byla jmenována tzv. CVE Numbering Authority (CNA), což svědčí o tom, že jako zodpovědný poskytovatel bezpečnostních řešení nepřetržitě vyhodnocuje a řeší nahlášené bezpečnostní zranitelnosti a incidenty. Naše produkty odpovídají požadavkům příslušných norem a legislativních předpisů, včetně PCI-DSS (finančnictví), HIPAA (zdravotnictví), CIPA (vzdělávání), nařízení GDPR a směrnice NIS2.



ZOBRAZIT KOMPLETNÍ ZPRÁVY ORGANIZACE TOLLY

Firewally Zyxel USG FLEX H versus Ubiquiti Dream Machine: hodnocení účinnosti ochrany proti malwaru

www.tolly.com/publications/225150

Zyxel USG FLEX 100H versus SonicWall TZ270: hodnocení účinnosti ochrany proti malwaru a srovnání nákladů na licence

www.tolly.com/publications/225151

Čím se lišíme od ostatních a proč na tom záleží

Společnost Zyxel Networks se od ostatních výrobců síťových technologií odlišuje tím, že je také uznávaným poskytovatelem řešení pro kybernetickou bezpečnost.

Žádná moderní firma se neobejde bez bezpečné a spolehlivé konektivity. Zyxel Networks je jednou z velmi mála společností, které dokáží malým a středně velkým firmám poskytnout bezpečnostní řešení splňující jejich nároky na jednoduchost, výkon a cenovou dostupnost.

S námi není kybernetická bezpečnost žádná věda

Bez ohledu na rostoucí složitost kybernetické bezpečnosti stále jdeme za stejným cílem: zajistit, aby kybernetická bezpečnost byla pro malé a středně velké firmy, prodejce IT a instalační firmy co nejjednodušší. Boříme bariéry, díky čemuž lze kybernetickou bezpečnost snáze pochopit i zajistit. Prosazujeme bezpečnostní řešení, která se rychle nasazují a snadno zdůvodňují, spravují a podporují.

Malým a středně velkým firmám poskytujeme komplexní řešení, které nedělá kompromisy v zabezpečení a které je neustále aktualizované a chráněné. IT a instalačním firmám nabízíme příležitost k posílení vztahů se zákazníky, k rozvoji podnikání a k získání opakovaných tržeb.



Copyright © 2026 Společnost Zyxel Networks a/nebo její přidružené společnosti.
Všechna práva vyhrazena. Veškeré specifikace podléhají změnám bez
předchozího upozornění. Navzdory maximální péči o zajištění přesnosti informací
obsažených v této publikaci společnost Zyxel Networks ani její dceřiné/přidružené
společnosti nepřebírají odpovědnost za případné chyby či nepřesnosti.

30/09/2026