**Zyxel Networks upraszcza bezpieczną łączność zdalną dzięki integracji z Tailscale**

**Nowe partnerstwo zapewnia prostą i łatwą usługę WireGuard VPN użytkownikom zapór sieciowych USG FLEX H bez dodatkowych kosztów.**

**Zyxel Networks**, lider w dostarczaniu bezpiecznych i opartych na sztucznej inteligencji rozwiązań sieciowych w chmurze, ogłosił dziś nowe partnerstwo z **Tailscale**, wiodącą platformą łączności natywnej dla tożsamości. Integracja ta zapewnia uproszczoną, skalowalną i bezpieczną łączność VPN z zaporami sieciowymi Zyxel Networks z serii **USG FLEX H**. Umożliwia małym firmom i zaawansowanym użytkownikom tworzenie prywatnych sieci peer-to-peer z łatwością i bez dodatkowych kosztów.

Dostępna teraz w zaporach sieciowych Zyxel Networks USG FLEX H z systemem operacyjnym uOS v1.32 lub nowszym, Tailscale WireGuard sieć VPN typu mesh jest w pełni zintegrowana z interfejsem zarządzania zapory sieciowej. Po włączeniu użytkownicy mogą skonfigurować bezpieczny dostęp zdalny w ciągu kilku minut, bez konieczności skomplikowanej konfiguracji.



**Usprawniona obsługa VPN**

Zapory sieciowe z serii USG FLEX H obsługują teraz pełen zestaw protokołów VPN, w tym IPSec, SSL i WireGuard, aby zabezpieczyć szerszy zakres przypadków użycia i punktów końcowych. Integracja Tailscale pozwala użytkownikom korzystać z usprawnionej konfiguracji,która nie wymaga konfiguracji serwera ani przekierowywania portów. Urządzenia mogą automatycznie łączyć się z siecią prywatną za pomocą kilku prostych kliknięć. Dzięki temu proces jest dostępny nawet dla osób z minimalnym doświadczeniem sieciowym.

**Chroniona kontrola dostępu**

Dzięki integracji z Tailscale użytkownicy zapór mogą teraz stworzyć sieć mesh peer-to-peer, w której urządzenia komunikują się ze sobą bezpośrednio za pośrednictwem szyfrowanych tuneli, zamiast routingu przez centralny serwer. Taka architektura zmniejsza opóźnienia, zwiększa wydajność i efektywnie skaluje się wraz z rozwojem firmy. Ponadto usługa obsługuje szeroką gamę systemów operacyjnych, w tym Windows, macOS, Linux, iOS i Android, a także urządzenia wbudowane i usługi w chmurze. Dzięki temu użytkownicy zapór sieciowych mogą rozszerzyć ochronę VPN na wszystkie główne punkty końcowe - w tym urządzenia przenośne i środowiska BYOD.

Dla większej wygody i bezpieczeństwa, użytkownicy mogą logować się do Tailscale korzystając ze swoich istniejących dostawców tożsamości, takich jak Google Workspace, Microsoft Entra ID (Azure AD), Okta, OneLogin czy JumpCloud. Dodatkowo przez te konta można wdrożyć uwierzytelnianie wieloskładnikowe (MFA). Zapewnia to dodatkową warstwę ochrony, jednocześnie upraszczając kontrolę dostępu i zarządzanie użytkownikami.

*Sieci VPN są niezbędne do ochrony danych i wspierania hybrydowej siły roboczej, ale często były zbyt skomplikowane dla mniejszych organizacji z ograniczonymi zasobami IT* - powiedział **Norbert Ogłoziński**, Country Sales Manager, Zyxel Networks Polska. *Ta integracja zapewnia naszym klientom prostszy, szybszy i inteligentniejszy sposób na włączenie bezpiecznych połączeń na wszystkich urządzeniach, gdziekolwiek się znajdują*.

*Sieci VPN mają reputację powolnych, bolesnych w konfiguracji i niemożliwych do zarządzania. Założyliśmy Tailscale, aby to naprawić, a teraz cieszymy się, że możemy zapewnić tę prostotę większej liczbie osób dzięki naszej współpracy z Zyxel Networks* - powiedział **Avery Pennarun**, współzałożyciel i dyrektor generalny Tailscale. *Zasięg Zyxel Networks na rynku SMB oznacza, że możemy pomóc znacznie większej liczbie zespołów pominąć "ból głowy VPN" i po prostu wrócić do pracy - bezpiecznie*.

W ramach partnerstwa Zyxel Networks oferuje kwalifikującym się klientom serii USG FLEX H bezpłatny dostęp do planu startowego Tailscale. Więcej informacji można znaleźć na stronie: <https://community.zyxel.com/en/discussion/29583>