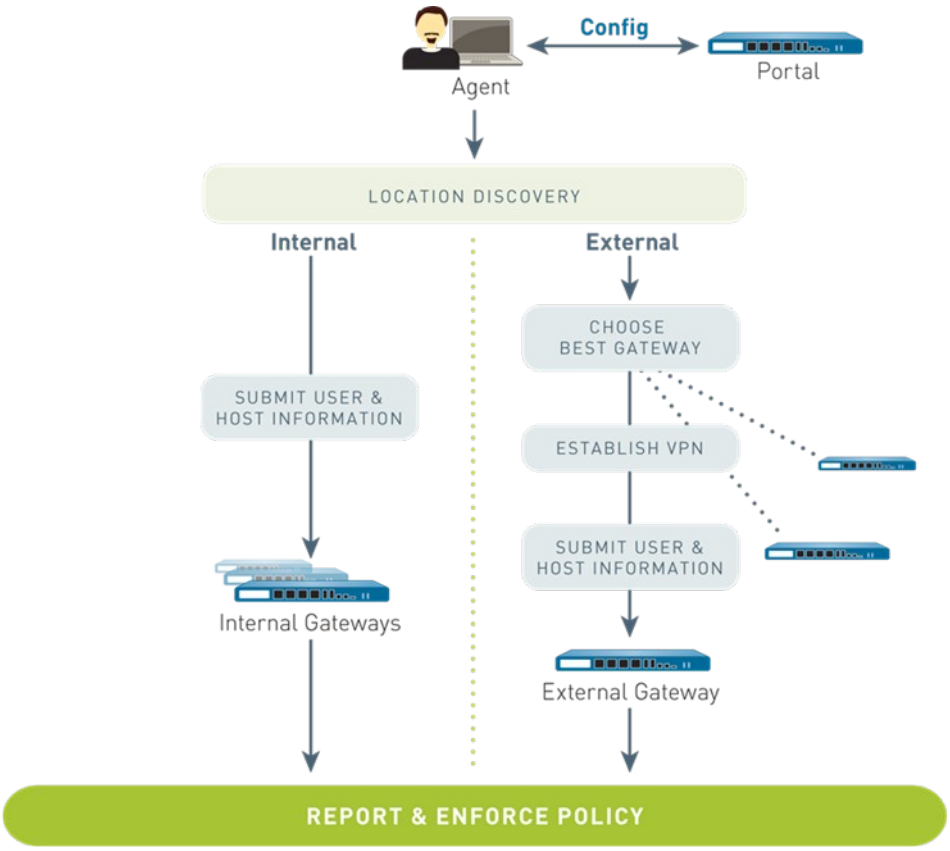
Global Protect - zdalny dostęp do zasobów

Global Protect to rozwiązanie zapewniające ochronę danych użytkowników niezależnie od ich fizycznej lokalizacji. Global Protect zapewnia ochronę użytkownikom mobilnym, niezależnie od tego czy znajdują się w: centrali firmy, w oddziale czy też w terenie. W skład Global Protect wchodzi oprogramowanie funkcjonujące na firewallach PaloAlto oraz oprogramowanie zainstalowany na końcówkach. *Agent (*Klient*)* zapewnia zestawienie bezpiecznego, szyfrowanego tunelu SSL/IPsec pomiędzy komputerem, tabletem lub smartphonem użytkownika a "najbliższym" gateway-em PaloAlto. Wybór gateway-a do którego podłączony zostanie użytkownik odbywa się w pełni automatycznie, zaś sama instalacja agenta może być zrealizowana u użytkownika automatycznie lub poprzez portal Global Protect.

Komponenty wchodzące w skład usługi GP:

- GlobalProtect Portal,
- GlobalProtect Gateway,
- GlobalProtect Client.



Rysunek 1 – zasady funkcjonowania klientów i bram GP

Global Protect może być wykorzystane zarówno do obsługi użytkowników *wewnętrznych* jak i *zewnętrznych* - dzięki serwisowi "***Location Discovery***" agent użytkownika określa swoją lokalizację względem bramy GP i łączy się odpowiednio albo z bramą wewnętrzną albo z jedną z bram zewnętrznych. W tym drugim wariancie dodatkowo zestawiany jest tunel VPN oraz badana i weryfikowana jest informacja o użytkowniku i jego urządzeniu (tzw. HIP). W każdym przypadku połączenie z GP podlega oczywiscie regułom określonym w polityce bezpieczeństwa.

GlobalProtect Portal

GlobalProtect Portal służy jako punkt połączenia klientów (użytkowników) z infrastrukturą.

Zadania GPP:

- Uwierzytelnia użytkowników inicjujących połączenie z usługą,
- Tworzy oraz przechowuje dedykowane konfiguracje dla klientów,
- Zarządza listą Internal oraz External Gateways,
- Zarządza certyfikatami CA służącymi do uwierzytelnienia.

GlobalProtect Portal – metody podłączenia

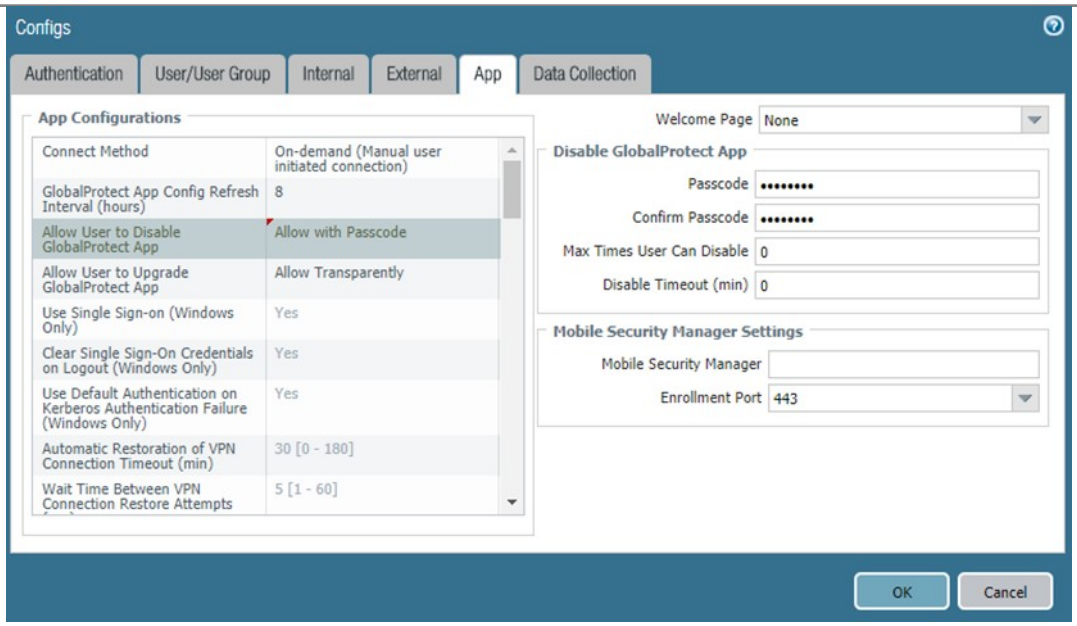
Klienci nie zawsze chcą i musza być połączeni do zasobów firmy poprzez GP, dlatego dostepne są trzy możliwości zestawienia bezpiecznego połączenia:

- **On-demand** – klient decyduje sam oraz kiedy chce zestawić tunel wykorzystując opcję Connect w agencie,
- **User-logon** – tunel zestawia się automatycznie w momencie uwierzytelnienia użytkownika na urządzeniu,
- **Pre-logon** – tunel zestawia się automatycznie przed uwierzytelnieniem użytkownika w urządzeniu - ten wariant jest konieczny, gdy uwierzytelneinie wymaga połączenia on-line z domeną, i gdy nie chcemy korzystać z cachowanych poświadczeń.

W konfiguracji GlobalProtect Portal administrator definiuje m.in.:

- Interfejs NGFW, na którym dostępny jest portal,
- Strony WWW portalu odpowiadające za: login, stronę pomocy i "landing page" (dostępne są oczywiscie wzorce),
- Metodę uwierzytelnienia (np. przez MS AD),
- Profil certyfikatów oraz profil SSL/TLS,
- Uwierzytelnienie użytkowników, np. certyfikat, 2FA - OTP, itd.
- Sposób detekcji klientów internal/external (bazując na rozwiązywaniu wewnetrznych adresów DNS),
- Opcje aplikacji GP na kliencie, parametry SSO, opcje auto-update-u, opcje deaktywacji aplikacji przez użytkownika i inne.

Warto zwrócić uwagę, że w przypadku użytkowników zewnętrznych, np. podróżujących po świecie właściwa dla danego użytkownika brama jest wybierana na podstawie zdefiniowanych kryteriów, tak aby klient łączył się z najbliższą (nie koniecznie w sensie dosłownym) bramą.

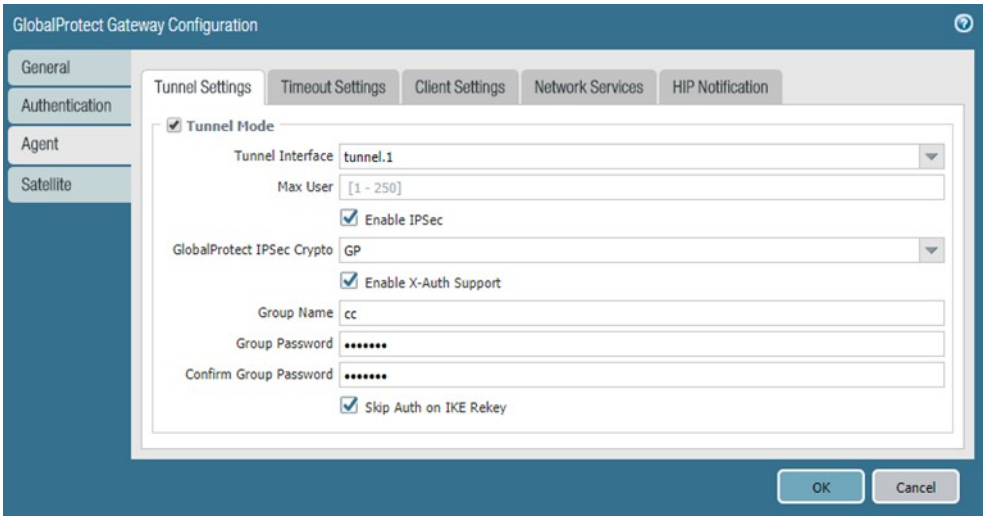


GlobalProtect Gateway

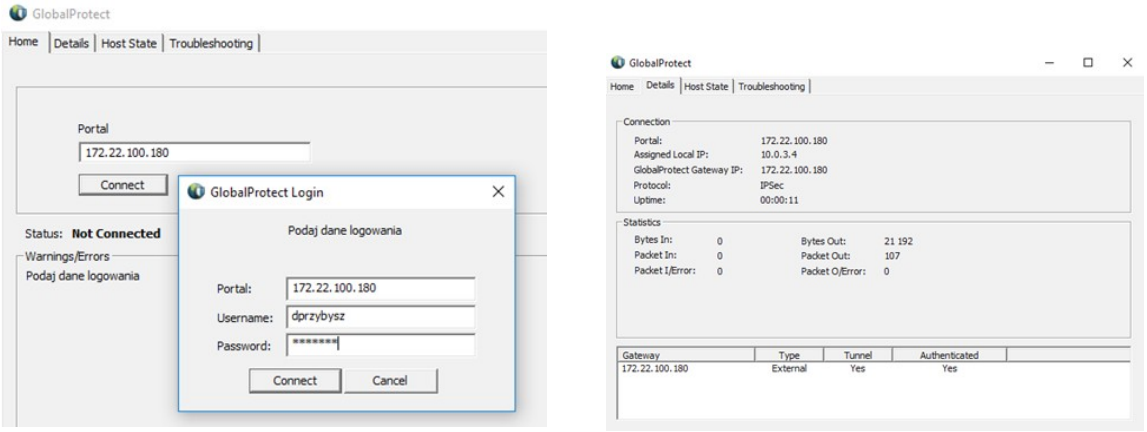
- Zapewnia bezpieczny przesył danych dla klientów moblinych,
- wymaga interfejsu tunelowego dla zewnętrznych klientów,
- interfejs tunelowy dla Internal Gateway jest opcjonalny.

W konfiguracji GlobalProtect Gateway określa się przede wszystkim parametry interfejsu tunelowego firewall-a oraz ***opcje*** połączenia ***VPN***. Możemy wybrać np. tunel ***SSL/TLS*** lub ***IPsec***, włączyć X-auth, itd. Definiujemy także róznorodne parametry tunelu takie jak czas życia, dozwolony czas niekatywności, reguły rutingu i zakresy adresacji IP; opcje DNS. Ustawienia te pozwalają na funkcjonowanie zewnętrznego klienta w trybie klienta VPN czyli wewnętrznego.

Domyślnie, w trakcie trwania połączenia VPN tunelowane jest 100% ruchu umożliwiając wgląd, inspekcję oraz szczegółową kontrolę ruchu nawiązywanego od użytkownika niezależnie od lokalizacji i używanego urządzenia. O ile jest to zalecane ze względów bezpieczeństwa, nie jest to jednak jedyna możliwość - jako administrator możemy podjąć decyzję jaki ruch ma podlegać tunelowaniu w oparciu o trasy routingowe (np. tunelowanie tylko adresacji prywatnych), domeny docelowe lub nawet specyficzna aplikacja (np. YouTube, Netflix). Pozwala to na wygodne sterowane ruchem oraz odciążenie łącza firmowego przez warunkowe wyłączenie określonej relacji z tunelu VPN bez jakiejkolwiek ingerencji ze strony użytkownika końcowego.



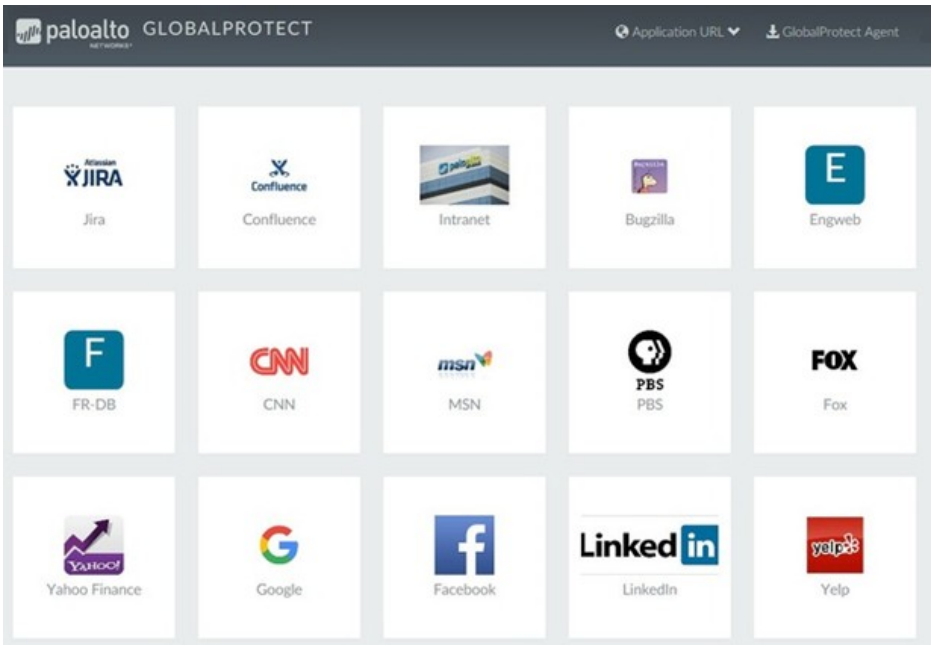
- GlobalProtect – Klient,
- wwierzytelnia użytkownika z portalem,
- zestawia tunel z bramą,
- wysyła raporty HIP,
- pozwala użytkownikom na różne poziomy zarządzania połączeniem.



Rysunek 2 – klient (agent) Global Protect

GlobalProtect Clientless VPN

Dostępny jest też wariant usługi ***GlobalProtect Clientless VPN***, który umożliwia bezpieczny, zdalny dostęp użytkowników do aplikacji webowych wykorzystujących HTML, HTML5 lub JavaScript. Zaletą tego rozwiązania jest wykorzystanie wyłącznie przeglądarki internetowej – nie jesteśmy zmuszeni do instalacji klienta na stacji końcowej.



Rysunek 3 – Przykładowy widok portalu Global Protect