VPN: tunel przez cudzy internet

Poziom: podstawy

Dotyczy: VPN, IPsec, IKEv2, SSL VPN (kontekst: FortiGate 100F i Windows)

Czas: ~15 min

Ta strona otwiera książkę o sieci i VPN: skąd wziął się pomysł szyfrowanego tunelu przez cudzą infrastrukturę, czym różnią się IPsec, IKE, IKEv2 i SSL VPN, oraz dlaczego Zielona bez VPN nie mogłaby wysłać handlowca w teren.

ZAŁOŻENIA SCENARIUSZA

ta opowieść wprowadza książkę i nie przyjmuje jednego układu sieci. Każda kolejna strona podaje własne założenia w takiej ramce: pojedynczy `fw01` albo para FortiGate, jedno łącze albo dwa ze Starlinkiem, magazyn w Swarzędzu w sieci centrali albo jako osobna lokalizacja z tunelem. Różnice między stronami są zamierzone.

Skróty użyte na tej stronie (15)

Skrót	Co znaczy
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IETF	Internet Engineering Task Force: organizacja publikująca standardy internetowe jako dokumenty RFC
IKE	Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec
IKEv2	Internet Key Exchange w wersji 2: nowsza odmiana IKE, wbudowana w klienta VPN Windows, szybciej wraca do życia po zerwaniu łącza niż starsze protokoły VPN
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
IPv6	Internet Protocol wersja 6: nowszy, dłuższy zapis adresów, w liczbach szesnastkowych oddzielonych dwukropkami

Skrót	Co znaczy
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
WMS	Warehouse Management System: system zarządzania magazynem

Skąd się wzięło

Na początku lat dziewięćdziesiątych firmy, które chciały połączyć dwa biura albo wpuścić pracownika z domu do sieci firmowej, miały do wyboru drogie łącze dzierżawione od operatora albo nic. Internet już istniał i był tani, ale ruch w nim płynął jawnie: każdy router po drodze mógł go przeczytać. Potrzebny był sposób, żeby przez tę wspólną, cudzą sieć poprowadzić prywatny, szyfrowany korytarz, tak jakby obie strony łączył kabel, którego nikt inny nie widzi.

Pierwszą szeroko znaną odpowiedzią był PPTP, protokół, nad którym w 1996 roku pracował zespół w Microsoft z Gurdeepem Singh-Pallem. Trafił od razu do Windows 95, więc słowo VPN wielu administratorów poznało właśnie z nim, choć jego szyfrowanie z dzisiejszej perspektywy uznaje się za słabe. Równolegle, w ramach prac nad IPv6, grupa robocza IETF rozwijała IPsec: zestaw reguł opisanych w RFC 1825 do 1829, opublikowanych w 1995 roku, dodający do zwykłego ruchu IP dwie rzeczy, których w nim brakowało: dowód, że pakiet nie został po drodze zmieniony, oraz jego szyfrowanie.

> **Pojęcie: IPsec.** Zestaw protokołów działających poniżej aplikacji, na poziomie samych pakietów IP, które szyfrują i podpisują ruch sieciowy tak, że aplikacja na końcu w ogóle nie wie, że coś takiego się dzieje.

Sam IPsec potrzebował jednak sposobu, żeby dwie strony w ogóle dogadały się co do klucza szyfrującego, zanim popłynie pierwszy bit danych. Tym zajął się IKE, opisany w 1998 roku w RFC 2409 przez Dana Harkinsa i Dave'a Carrela, łączący wcześniejszy protokół ISAKMP z metodami wymiany kluczy Oakley i SKEME. IKE działał, ale wymagał wielu wiadomości w obie strony i słabo radził sobie, gdy laptop zmieniał sieć, na przykład z Wi-Fi na kartę SIM. W 2005 roku, w RFC 4306, uproszczono go do IKEv2: mniej wiadomości, wbudowana obsługa NAT po drodze i mechanizm

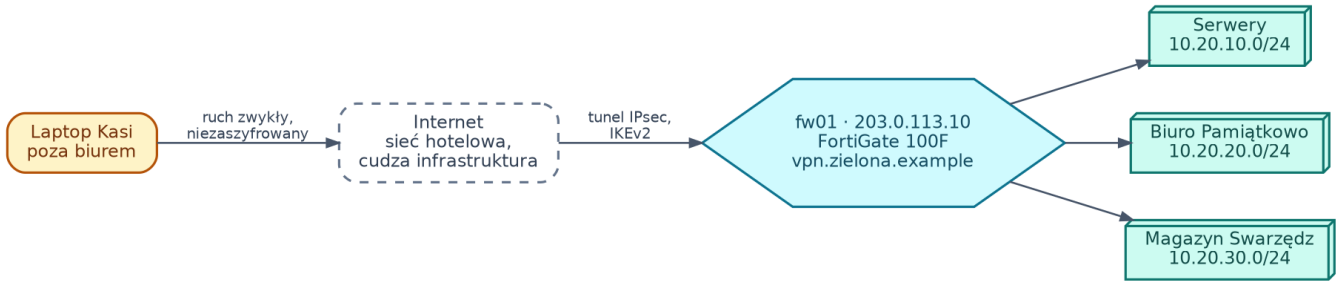
MOBIKE, pozwalający tunelowi przeżyć zmianę adresu IP klienta bez zrywania połączenia. To ostatnie jest powodem, dla którego dzisiejszy wbudowany klient VPN Windows stawia właśnie na IKEv2.

Mniej więcej w tym samym czasie, w połowie lat dwutysięcznych, pojawiła się trzecia rodzina rozwiązań: SSL VPN. Zamiast osobnego protokołu na poziomie pakietów IP, tunel prowadzono przez zwykłe połączenie TLS, często na porcie 443, tym samym, którym przegląda się strony HTTPS. Taki tunel bez trudu przechodził przez firmowe zapory i hotelowe portale logowania, które i tak przepuszczają ruch do stron internetowych. Kosztem był brak dostępu do niektórych niżej poziomowych sztuczek IPsec, ale zyskiem: łatwość wdrożenia tam, gdzie IPsec utykał na jakimś pośrednim urządzeniu sieciowym.

Jak to działa w jednym obrazku

> **Pojęcie: VPN.** Virtual Private Network, czyli sieć prywatna zbudowana nie z własnych kabli, tylko z szyfrowanego tunelu poprowadzonego przez sieć, która do nas nie należy, najczęściej internet.

> **Pojęcie: tunel.** Sposób przesyłania danych, w którym cały oryginalny pakiet zostaje zamknięty, zaszyfrowany i opakowany w nowy pakiet na czas podróży przez sieć pośredniczącą. Na drugim końcu tunelu opakowanie znika, a odbiorca dostaje oryginalny pakiet, tak jakby przyszedł prosto z lokalnej sieci.



Mapa drogi ruchu VPN: laptop w terenie przez internet do bramy fw01, dalej do sieci Zielonej (kliknięcie otwiera pełny rozmiar)

Trzy rodziny protokołów z poprzedniej sekcji różnią się tym, na jakim poziomie budują ten tunel. IPsec z IKEv2 pracuje nisko, na poziomie samych pakietów IP, i obejmuje każdy ruch z laptopa, niezależnie od aplikacji. SSL VPN pracuje wyżej, wewnątrz połączenia TLS, i bywa ograniczony tylko

do wybranych aplikacji albo stron. W Zielonej na stacjach Windows stoi wbudowany klient IKEv2, bo nie wymaga instalowania niczego dodatkowego i przechodzi bezproblemowo zmianę sieci w trakcie podróży handlowca.

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Kasia, handlowiec w terenie, siedzi w hotelu w Krakowie o 21:00 dzień przed spotkaniem z klientem. Potrzebuje otworzyć w Optimie fakturę sprzed tygodnia i sprawdzić stan magazynowy w WMS, zanim rano pojedzie na spotkanie. Hotelowe Wi-Fi to sieć współdzielona z dziesiątkami obcych gości, więc zwykłe połączenie do serwera w Pamiątkowie byłoby widoczne dla każdego w tej samej sieci.

Bez VPN zespół IT Zielonej miałby dwie złe opcje: wystawić Optimę, WMS i udziały plikowe wprost do internetu, licząc na samo hasło jako jedyną obronę, albo zabronić pracy zdalnej i zmusić Kasię do powrotu do biura po każdą fakturę. Żadna z tych opcji nie wytrzymuje starcia z audytem pana Wojtka, który raz w roku pyta właśnie o to, kto i skąd ma dostęp do systemów firmowych.

VPN rozwiązuje to inaczej: `fw01`, FortiGate 100F stojący na styku sieci Zielonej z internetem, wystawia jeden, dobrze zabezpieczony punkt wejścia pod adresem `vpn.zielona.example`. Laptop Kasi łączy się z tym punktem tunelem IKEv2, a dopiero z drugiej strony tunelu, tak jakby siedziała w biurze w Pamiątkowie, dociera do Optimy na `sql01` i do WMS na `ora01`. Żaden z tych serwerów nigdy nie jest bezpośrednio widoczny z internetu.

Mapa tej książki

Strona	Na jakie pytanie odpowiada
01. Opowieść	Skąd wziął się VPN i dlaczego Zielona bez niego nie wysłałaby nikogo w teren
02. IPsec i IKEv2 po ludzku	Jak dwie strony tunelu dogadują się co do szyfrowania, zanim popłyną dane
03. Błąd 13801	Dlaczego Windows odrzuca certyfikat bramy VPN i jak wystawić poprawny
04. AlwaysOn VPN	Jak wdrożyć tunel użytkownika przez ProfileXML, bez klikania w interfejs na każdym laptopie
05. EAP-TLS i FSSO	Jak zalogować się do VPN certyfikatem użytkownika i dostać dostęp do zasobów według grup z Active Directory

Strona	Na jakie pytanie odpowiada
FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT	Jak zarządzamy siecią na FortiGate: interfejsy, VLAN-y, polityki, NAT i aktualizacje
Para FortiGate w klastrze: FGCP aktywny-pasywny	Jak zrobić z dwóch FortiGate klaster, żeby zapora przestała być pojedynczym punktem awarii
IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy	Jak połączyć Pamiątkowo ze Swarzędzem tunelem IPsec między FortiGate a routerem innej firmy, z zapasem przez Starlink
IPsec dla pracowników: FortiClient i dial-up IKEv2 na FortiGate	Jak pracownicy łączą się przez IPsec z FortiClient albo wbudowanym klientem Windows
SSL VPN i ZTNA: co z SSL VPN w nowych FortiOS i czym go zastąpić	Co się stało z SSL VPN w nowych FortiOS i czym go zastąpić
WireGuard i OpenVPN: odpowiedniki spoza FortiGate na Linuksie	Czym są WireGuard i OpenVPN na Linuksie i kiedy wybrać je zamiast IPsec

Częste błędy

Objaw	Przyczyna	Co robimy
„VPN załatwia bezpieczeństwo, więc reszta się nie liczy"	VPN szyfruje tylko drogę między laptopem a `fw01`, nic więcej	traktujemy VPN jako jeden z kilku elementów obrony, obok haseł, uprawnień i aktualizacji
Mylenie SSL VPN z IPsec VPN jako tego samego rozwiązania	obie rodziny nazywa się potocznie „VPN", choć różnią się warstwą i sposobem działania	sprawdzamy w dokumentacji urządzenia, którą rodzinę faktycznie skonfigurowano, zanim szukamy przyczyny awarii
Przekonanie, że pełny tunel (full tunnel) jest zawsze bezpieczniejszy niż split tunnel	pełny tunel kieruje przez `fw01` również ruch do zwykłych stron internetowych, co obciąża łącze biura i samą zaporę	wybieramy zakres tunelowania świadomie, zależnie od tego, czego naprawdę trzeba bronić, temat rozwijamy na kolejnej stronie

□□ Ćwiczenia

1. Kasia loguje się do VPN z hotelu, a potem otwiera w przeglądarce zwykłą stronę z wiadomościami. Czy ten drugi ruch też przechodzi przez `fw01`?

Odpowiedź

Zależy od trybu tunelowania. Przy pełnym tunelu (full tunnel) cały ruch, także do zwykłych stron, wraca przez `fw01`. Przy split tunnelu przez `fw01` wraca tylko ruch do sieci Zielonej, a strona z wiadomościami idzie prosto z hotelowego Wi-Fi do internetu, z pominięciem tunelu.

1. Dlaczego wbudowany klient VPN Windows korzysta z IKEv2, a nie ze starszego IKE?

Odpowiedź

IKEv2 wymaga mniej wiadomości do zestawienia tunelu i ma wbudowany mechanizm MOBIKE, pozwalający tunelowi przetrwać zmianę sieci klienta, na przykład przejście z Wi-Fi hotelowego na kartę SIM w trakcie podróży, bez zrywania połączenia.

Źródła: en.wikipedia.org/wiki/Virtual_private_network · en.wikipedia.org/wiki/IPsec · datatracker.ietf.org/doc/html/rfc2409 (IKE) · datatracker.ietf.org/doc/html/rfc4306 (IKEv2) · en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol · en.wikipedia.org/wiki/OpenVPN

Revision #27
Created 2026-09-28 06:15:08 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:07 UTC by Tomasz Konieczny