IPsec i IKEv2 po ludzku: fazy, propozycje, uwierzytelnianie

Poziom: podstawy **Dotyczy: FortiGate 100F (FortiOS 7.4/7.6), Windows 11**

Czas: ~25 min

Zanim dwie strony tunelu VPN wymienią pierwszy zaszyfrowany pakiet, muszą się dogadać co do szyfru, skrótu i sposobu, w jaki się sobie nawzajem udowodnią, że są tym, za kogo się podają. Ta strona pokazuje, jak wygląda ta rozmowa i gdzie najczęściej się psuje.

ZAŁOŻENIA SCENARIUSZA

tunel kończy się na pojedynczym `fw01` (FortiGate 100F) w centrali, na `wan1` z adresem 203.0.113.10, a Zielona ma w przykładach jedno łącze światłowodowe. Wariant z parą FortiGate opisuje Para FortiGate w klastrze: FGCP aktywny-pasywny, a wariant z drugim łączem ze Starlinkiem Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate.

Skróty użyte na tej stronie (10)

Skrót	Co znaczy
AES256	konkretny wariant szyfru AES z kluczem o długości 256 bitów
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
EAP	Extensible Authentication Protocol: rodzina metod uwierzytelniania, dzięki której VPN albo Wi-Fi mogą pytać o hasło albo o certyfikat na wiele różnych sposobów
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
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
SHA1	starsza, dziś uznawana za słabą funkcja skrótu kryptograficznego
SHA256	funkcja skrótu kryptograficznego dająca 256-bitowy odcisk danych

Skrót	Co znaczy
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

TYLKO ODCZYT

Sprawdzenie stanu bram IKE: diagnose vpn ike gateway list

```
diagnose vpn ike gateway list
```

Pokazuje stan negocjacji fazy 1 dla każdej bramy IKE skonfigurowanej na `fw01`: adres zdalny, wersję IKE, liczbę utworzonych i ustanowionych SA. Sięgamy po nią jako pierwszą komendę, gdy tunel w ogóle nie wstaje.

Przykład:

```
vd: root/0
name: vpn.zielona.example
version: 2
interface: wan1 9
addr: 203.0.113.10:4500 -> 203.0.113.33:37652
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
```

IKE = Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Włączenie szczegółowego debugu IKE: diagnose debug application ike -1

```
diagnose debug application ike -1
```

Ustawia najwyższy poziom szczegółowości logów negocjacji IKE (wartość `-1` oznacza wszystkie kategorie). Sama ta komenda jeszcze niczego nie pokazuje na ekranie, dopiero kolejna fiszka włącza wypisywanie.

IKE = Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Włączenie wypisywania logów debug na konsolę: diagnose debug enable

```
diagnose debug enable
```

Włącza wysyłanie wcześniej włączonych logów debug na bieżącą sesję CLI. Dopiero po tej komendzie zaczynamy widzieć na ekranie przebieg negocjacji IKE ustawiony fiszką wyżej, na przykład w momencie, gdy Kasia z hotelu próbuje połączyć się z `vpn.zielona.example`.

Przykład:

```
ike 0: comm_recv: IKEv2 exchange=IKE_SA_INIT id=... len=464
ike 0:vpn.zielona.example:226: no SA proposal chosen
ike 0:vpn.zielona.example:226: negotiation failure
```

> Wyłączamy debug tą samą parą poleceń z flagą przeciwną: `diagnose debug application ike 0` i `diagnose debug disable`, żeby konsola nie zalewała się logami po zakończonej diagnozie.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu · **IKE** = Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Podsumowanie stanu tuneli IPsec: get vpn ipsec tunnel summary

```
get vpn ipsec tunnel summary
```

Jednowierszowe podsumowanie każdego tunelu IPsec: adresy obu stron, liczbę aktywnych selektorów i liczniki pakietów. Krótsza wersja tego, co pokazuje `diagnose vpn ike gateway list`, przydatna do szybkiego rzutu oka na kilka tuneli naraz.

Przykład:

```
'vpn.zielona.example' 203.0.113.10:0 -> 203.0.113.33:0 selectors(total,up): 1/1
rx(pkts,errs): 842/0 tx(pkts,errs): 917/0
```

IPsec = Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2 · **get** = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

Z życia wzięte

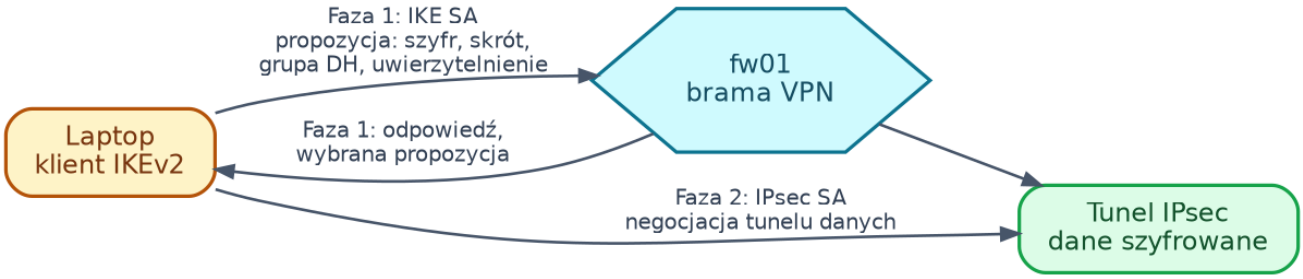
Z ŻYCIA WZIĘTE

Tomek, drugi tydzień pracy, dostaje zgłoszenie od Kasi: „VPN się nie łączy, siedzę w hotelu, jutro mam spotkanie". Otwiera CLI na `fw01` i odpala `diagnose vpn ike gateway list`, ale wpisu dla adresu Kasi w ogóle nie widzi, jakby próba połączenia nie dotarła dalej niż pierwsza wymiana. Włącza `diagnose debug application ike -1` razem z `diagnose debug enable` i prosi Kasię, żeby spróbowała jeszcze raz.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: Faza 1 (IKE SA). Pierwszy etap rozmowy dwóch stron tunelu, w którym ustalają, jakim szyfrem i jakim skrótem będą chronić dalszą rozmowę, oraz udowadniają sobie nawzajem tożsamość. Dopiero po zakończeniu fazy 1 obie strony mają wspólny, bezpieczny kanał, którym mogą negocjować dalej.



Dwie fazy negocjacji IKEv2: faza 1 ustala klucze i tożsamość, faza 2 otwiera tunel danych (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: Faza 2 (IPsec SA, czasem Child SA).** Drugi etap, prowadzony już wewnątrz bezpiecznego kanału z fazy 1, w którym strony ustalają osobny komplet kluczy do szyfrowania właściwych danych użytkownika. To dopiero po fazie 2 płyną pakiety Kasi do Optimy czy WMS.

> **Pojęcie: propozycja.** Zestaw trzech wyborów zgłaszanych przez każdą ze stron: algorytm szyfrujący (na przykład AES256), algorytm skrótu używany do podpisu i integralności (na przykład SHA256) oraz grupa Diffie-Hellman do wymiany klucza. Obie strony muszą zgodzić się na dokładnie jeden wspólny zestaw tych trzech wartości, osobno dla fazy 1 i osobno dla fazy 2, inaczej negocjacja kończy się błędem „no matching proposal" widocznym w przykładzie fiszki wyżej.

> **Pojęcie: grupa Diffie-Hellman (DH).** Numer opisujący, jak dużą i jak bezpieczną matematyczną łamigłówkę obie strony rozwiązują, żeby ustalić wspólny tajny klucz bez wysyłania go wprost przez sieć. Wyższy numer grupy zwykle oznacza mocniejsze zabezpieczenie kosztem odrobiny więcej obliczeń przy zestawianiu tunelu.

Trzy sposoby, w jaki strony tunelu mogą sobie dowieść tożsamości w fazie 1, różnią się tym, co dokładnie sprawdzają:

Metoda	Co sprawdza	Kiedy pasuje
PSK (Pre-Shared Key)	obie strony znają to samo, wcześniej ustalone hasło	proste tunele między dwiema stałymi bramami, mało kont
Certyfikat	strona przedstawia certyfikat podpisany przez zaufany urząd certyfikacji	brama zawsze uwierzytelnia się certyfikatem serwera, klient może uwierzytelniać się certyfikatem maszyny albo użytkownika

Metoda	Co sprawdza	Kiedy pasuje
EAP	użytkownik podaje hasło albo certyfikat przez dodatkową wymianę wewnątrz IKE, sprawdzaną przez serwer RADIUS albo lokalnie	logowanie osoby, nie samego urządzenia, na przykład wpisywane hasło domenowe przy każdym połączeniu

> ⚠ W jednym tunelu IKEv2 uwierzytelnienie EAP i uwierzytelnienie certyfikatem maszyny wzajemnie się wykluczają. Wbudowany profil VPN Windows definiuje albo `MachineMethod` z certyfikatem (tunel urządzenia), albo `UserMethod` z EAP lub certyfikatem użytkownika (tunel użytkownika), nigdy oba naraz w tej samej negocjacji. To ograniczenie samego mechanizmu, nie błąd konfiguracji, więc zmiana metody uwierzytelniania wymaga zmiany profilu, nie tylko dopisania drugiej opcji obok pierwszej.

Pojęcie: split tunnel i full tunnel. Split tunnel wysyła przez VPN wyłącznie ruch do sieci firmowej, a ruch do zwykłych stron internetowych idzie prosto z lokalnej sieci klienta. Full tunnel wysyła przez VPN cały ruch klienta, łącznie z przeglądaniem stron, co daje firmie pełną kontrolę i widoczność kosztem obciążenia łącza biura. Zielona korzysta ze split tunnelu: trasy do trzech sieci `10.20.10.0/24`, `10.20.20.0/24` i `10.20.30.0/24` idą przez `fw01`, reszta ruchu Kasi zostaje na miejscu.

Częste błędy

Objaw	Przyczyna	Co robimy
Negocjacja kończy się natychmiast błędem „no matching proposal chosen" w fazie 1	fw01 i klient mają skonfigurowaną inną grupę Diffie-Hellman w fazie 1, na przykład grupa 14 po jednej stronie i grupa 19 po drugiej	ujednolicamy listę dopuszczonych grup DH po obu stronach, sprawdzając ją w `diagnose debug application ike -1`
Faza 1 kończy się sukcesem, ale faza 2 (dane) w ogóle nie wstaje	niezgodność algorytmu skrótu w fazie 2, klasycznie SHA1 po jednej stronie i SHA256 po drugiej	wyrównujemy zestaw propozycji fazy 2 po obu stronach, usuwając SHA1 tam, gdzie jest wciąż dopuszczony ze starszej konfiguracji
Klient z profilem EAP nie łączy się z bramą skonfigurowaną tylko pod certyfikat maszyny	próba połączenia tunelem urządzenia (`MachineMethod`) do bramy oczekującej EAP, albo odwrotnie	sprawdzamy, czy profil klienta i konfiguracja `fw01` używają tej samej metody uwierzytelniania z tabeli wyżej

Objaw	Przyczyna	Co robimy
`diagnose vpn ike gateway list` w ogóle nie pokazuje wpisu dla adresu klienta	pierwsza wiadomość IKE nie dotarła do `fw01`, zwykle port UDP 500 albo 4500 zablokowany po drodze, na przykład przez hotelowe Wi-Fi	sprawdzamy zaporę hotelową i firmową na obu portach, zanim szukamy przyczyny w samej konfiguracji IKE

Ćwiczenia

1. Diagnoza `diagnose vpn ike gateway list` pokazuje `IKE SA: created 1/1 established 1/1`, ale `IPsec SA: created 0/1 established 0/0`. W której fazie jest problem?

Odpowiedź

Problem jest w fazie 2. Faza 1 (IKE SA) zakończyła się poprawnie, obie strony mają już bezpieczny kanał i potwierdzoną tożsamość, ale negocjacja fazy 2 (IPsec SA), czyli właściwego tunelu danych, się nie powiodła, najczęściej przez niezgodność propozycji fazy 2, na przykład SHA1 kontra SHA256.

1. Dlaczego Windows nie pozwala połączyć w jednym profilu VPN uwierzytelnienia EAP z uwierzytelnieniem certyfikatem maszyny?

Odpowiedź

Bo profil VPNv2 rozróżnia dwa oddzielne tunele: urządzenia (`MachineMethod`, zawsze certyfikat) i użytkownika (`UserMethod`, EAP albo certyfikat użytkownika). Te dwie metody odpowiadają dwóm różnym pytaniom: „czy to zaufany sprzęt firmy" i „czy to zalogowana, uprawniona osoba", więc mechanizm nie miesza ich w jednej negocjacji tego samego tunelu.

Źródła: IKE and IPsec monitoring, Fortinet Document Library · RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2) · VPNv2 CSP, Microsoft Learn

---

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