IPsec dla pracowników: FortiClient i dial-up IKEv2 na FortiGate

Poziom: zaawansowany

Dotyczy: FortiGate 100F (FortiOS 7.4/7.6), FortiClient 7.4 i 8.0, wbudowany klient VPN Windows 11, NPS na Windows Server 2022 (dc02)

Czas: ~50 min

Pracownik w terenie łączy się z `fw01` tunelem IPsec typu dial-up, czyli takim, w którym brama nie zna z góry adresu klienta. Strona pokazuje, jak wygląda ten tunel po stronie FortiGate, czym różni się klient FortiClient od wbudowanego klienta Windows i gdzie wchodzą RADIUS, NPS i drugi składnik logowania. Wracamy tu, gdy przybywa nowa grupa użytkowników albo gdy ktoś pyta, czy kupujemy FortiClient.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu brama VPN `vpn.zielona.example` pracuje normalnie na `wan1` z adresem 203.0.113.10, a Starlink na `wan2` ma publiczny, ale zmienny adres (203.0.113.30 w innych miejscach książki to tylko przykład). Dlatego w profilach klientów nie wpisujemy żadnego numeru, tylko nazwę, a po awarii `wan1` nazwa musi zacząć wskazywać aktualny adres `wan2` albo stały adres punktu zaczepienia w chmurze, jak opisuje strona Łącza operatora. Na innych stronach książki łącze zapasowe bywa pokazane prościej, co jest zamierzoną różnicą.

Skróty użyte na tej stronie (28)

Skrót	Co znaczy
2FA	Two Factor Authentication, dwuetapowe logowanie: drugi składnik logowania obok hasła głównego, na przykład kod z aplikacji uwierzytelniającej albo klucz sprzętowy
DDNS	Dynamic DNS: usługa, w której zapora sama zgłasza dostawcy DNS nowy adres, gdy się zmieni, więc nazwa nadal wskazuje aktualny adres; używamy jej przy łączu ze zmiennym adresem, na przykład ze Starlinka
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

Skrót	Co znaczy
EAP	Extensible Authentication Protocol: rodzina metod uwierzytelniania, dzięki której VPN albo Wi-Fi mogą pytać o hasło albo o certyfikat na wiele różnych sposobów
EAP-TLS	EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła
EKU	Extended Key Usage: pole w certyfikacie mówiące, do czego wolno go używać, na przykład wyłącznie do uwierzytelniania serwera
FSSO	Fortinet Single Sign-On: mechanizm FortiGate, który podgląda logowania w Active Directory i sam wie, z jakiej grupy korzysta dana osoba, bez proszenia jej o dodatkowe hasło
IKE	Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec
IKEv1	Internet Key Exchange w wersji 1: starsza wersja negocjacji tunelu IPsec, wycofywana z nowszych klientów na rzecz IKEv2
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
LAN	Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol w wersji 2: metoda sprawdzania hasła w sieci, używana wewnątrz PEAP
NAT	Network Address Translation: podmiana adresów IP na granicy sieci
NAT-T	NAT Traversal: opakowanie ruchu IPsec w UDP na porcie 4500, żeby przeszedł przez router z NAT, który nie przepuszcza ESP
NPS	Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi
PEAP	Protected EAP: odmiana EAP, która najpierw zestawia szyfrowany tunel TLS, a dopiero w nim przesyła hasło użytkownika
RADIUS	Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne
RMM	Remote Monitoring and Management: platforma do zdalnego zarządzania i monitorowania stacji roboczych
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TOTP	Time based One Time Password: jednorazowy kod zmieniający się co chwilę, generowany przez aplikację uwierzytelniającą jako jedna z metod dwuetapowego logowania
TPM	Trusted Platform Module: układ w komputerze, który przechowuje klucze szyfrowania i potwierdza stan sprzętu, między innymi dla BitLockera i certyfikatów

Skrót	Co znaczy
TTL	Time To Live: czas życia rekordu lub danych
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
ZTNA	Zero Trust Network Access: dostęp do pojedynczych aplikacji po sprawdzeniu użytkownika i stanu jego urządzenia, bez wpuszczania do całej sieci

Fiszka

Komendy FortiOS wykonujemy na `fw01`, komendy PowerShell na `dc02`. Sam tunel z uwierzytelnianiem EAP-TLS i grupami FSSO opisuje strona EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD, a profil klienta Windows strona AlwaysOn VPN: tunel użytkownika z ProfileXML. Tutaj dokładamy to, czego tam brakuje: pulę adresów, zasięg tunelu, RADIUS i porównanie klientów.

□□ TYLKO ODCZYT

Test logowania na serwerze RADIUS: diagnose test authserver radius

```
diagnose test authserver radius NazwaSerweraRadius mschap2 nazwa_usera HasloUzytkownika
```

Wysyła z `fw01` żądanie uwierzytelnienia do serwera RADIUS tak, jakby logował się użytkownik, więc sprawdzamy nią sam NPS bez udziału klienta VPN [1]. Metodę (`pap`, `chap`, `mschap`, `mschap2`) dobieramy do tego, czego używa tunel.

Przykład (skrócony, poglądowy):

```
authenticate 'jan.nowak' against 'mschap2' succeeded, server=primary
assigned_rad_session_id=1190820099
```

□□ **RADIUS** = Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne · **NPS** = Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

TYLKO ODCZYT

Podgląd uwierzytelniania na FortiGate: diagnose debug application fnbamd -1

```
diagnose debug application fnbamd -1
diagnose debug enable
```

Pokazuje rozmowę zapory z serwerem RADIUS: wysłane żądanie, odpowiedź `Access-Accept` albo `Access-Reject` i dopasowanie do grup. Wyłączamy komendami `diagnose debug disable` i `diagnose debug reset`.

RADIUS = Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

ZMIENIA SYSTEM

Definicja serwera RADIUS i grupy: config user radius

```
config user radius
    edit "NPS_dc02"
        set server "10.20.10.12"
        set secret HasloRadiusNps
        set auth-type auto
        set timeout 60
        set nas-ip 10.20.10.1
    next
end
config user group
    edit "VPN_Zielona_Uzytkownicy"
        set member "NPS_dc02"
    next
end
```

Rejestruje NPS z `dc02` jako serwer RADIUS i buduje grupę `VPN_Zielona_Uzytkownicy`, której członkiem jest ten serwer, więc każdy użytkownik zaakceptowany przez NPS należy do tej grupy. Kto z domeny w ogóle zostanie zaakceptowany, rozstrzyga zasada sieciowa NPS z członkostwem w `GG_VPN_Uzytkownicy`. Timeout 60 sekund wynika z zalecenia Microsoft dla serwera VPN współpracującego z rozszerzeniem NPS i MFA [2].

RADIUS = Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne · **NPS** = Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **MFA** = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu

ZMIENIA SYSTEM

Dodanie fw01 jako klienta RADIUS w NPS: New-NpsRadiusClient

```
New-NpsRadiusClient -Name "fw01" -Address "10.20.10.1" -SharedSecret "HasloRadiusNps"
```

Dopisuje `fw01` jako klienta RADIUS w NPS na `dc02`. Wspólny sekret musi być identyczny z `secret` w `config user radius`, a wpis może też powstać w konsoli NPS [3].

RADIUS = Remote Authentication Dial-In User Service: standardowy protokół pytania serwera, czy podane konto i hasło są poprawne · **NPS** = Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi

ZMIENIA SYSTEM

Przydział adresów, DNS i zasięgu tunelu: config vpn ipsec phase1-interface

```
config firewall address
    edit "SIEC_10"
        set subnet 10.20.10.0 255.255.255.0
    next
    edit "SIEC_20"
        set subnet 10.20.20.0 255.255.255.0
    next
    edit "SIEC_30"
        set subnet 10.20.30.0 255.255.255.0
    next
    edit "VPN_PULA"
        set subnet 10.20.200.0 255.255.255.0
    next
end
config firewall addrgrp
    edit "ZIELONA_SIEC"
```

```
        set member "SIEC_10" "SIEC_20" "SIEC_30"
    next
end
config vpn ipsec phase1-interface
    edit "vpn_zielona_user"
        set mode-cfg enable
        set ipv4-start-ip 10.20.200.10
        set ipv4-end-ip 10.20.200.250
        set ipv4-netmask 255.255.255.0
        set dns-mode manual
        set ipv4-dns-server1 10.20.10.11
        set ipv4-dns-server2 10.20.10.12
        set domain "ad.zielona.example"
        set ipv4-split-include "ZIELONA_SIEC"
    next
end
```

Dopisuje do tunelu `vpn_zielona_user` ze strony o EAP-TLS pulę 10.20.200.10 do 10.20.200.250, serwery DNS i listę sieci, które klient ma kierować do tunelu (split tunnel) [4]. Pozostałych ustawień tunelu (EAP, certyfikat bramy, grupa) nie ruszamy.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **EAP-TLS** = EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła · **EAP** = Extensible Authentication Protocol: rodzina metod uwierzytelniania, dzięki której VPN albo Wi-Fi mogą pytać o hasło albo o certyfikat na wiele różnych sposobów

KLIKAMY W INTERFEJSIE

Dodanie połączenia w FortiClient: Configure VPN

```
FortiClient → Remote Access → Configure VPN → IPsec VPN
Connection Name: Zielona VPN
Remote Gateway: vpn.zielona.example
Authentication Method: zgodnie z tunelem (EAP albo certyfikat)
```

Tworzy w kliencie połączenie z bramą `vpn.zielona.example`. Nazwy pól różnią się między wersjami FortiClient, więc sprawdzamy je w naszej wersji.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: okno Configure VPN w FortiClient z typem IPsec VPN, nazwą Zielona VPN i bramą `vpn.zielona.example`, z widocznym polem metody uwierzytelniania.

VPN = Virtual Private Network: szyfrowany tunel do sieci firmowej · **IPsec** = Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2

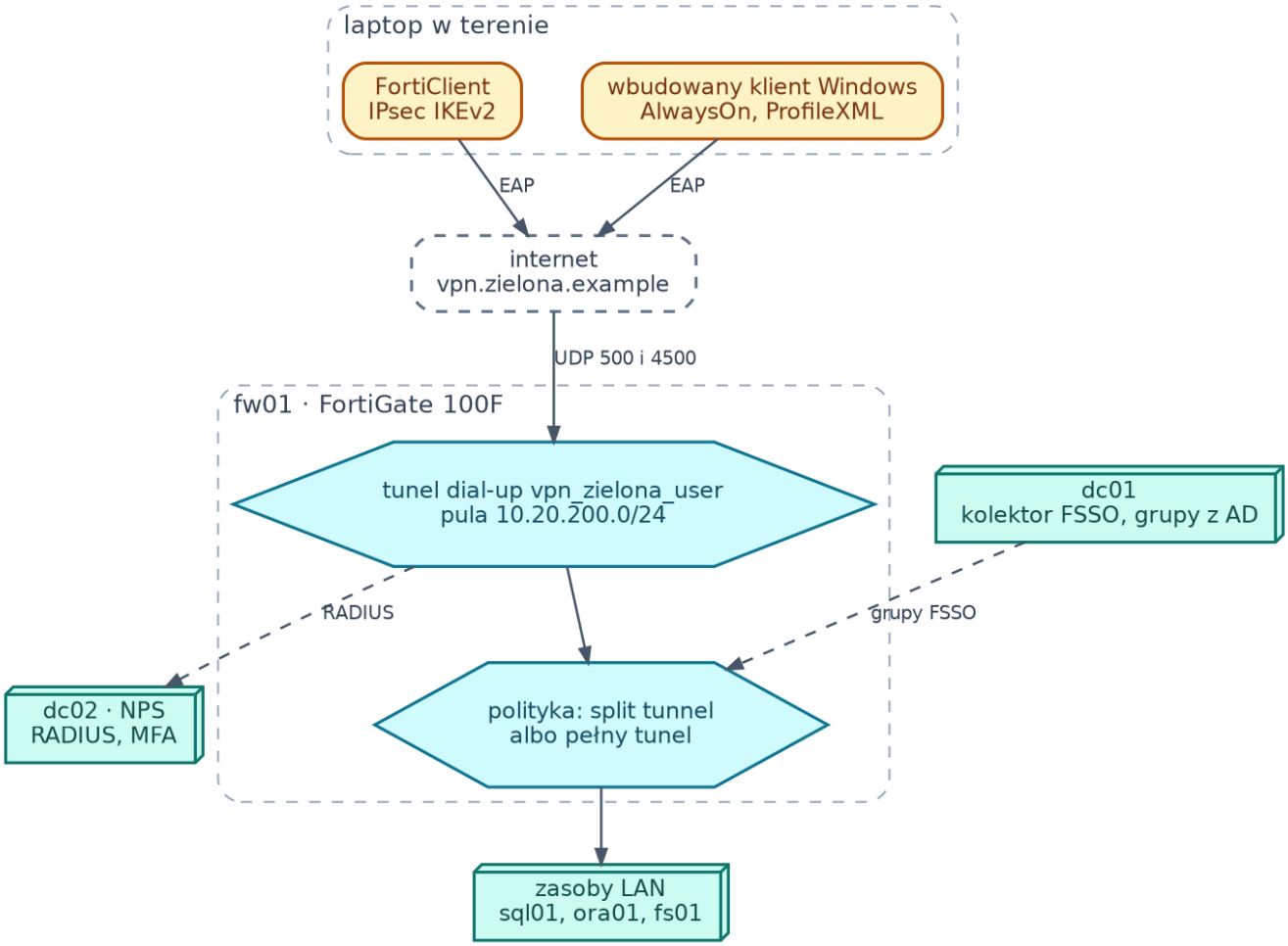
Z życia wzięte

Z ŻYCIA WZIĘTE

Piątek, 8:30. Kasia w pociągu do Wrocławia próbuje połączyć się z VPN, dostaje powiadomienie w aplikacji do potwierdzenia logowania, ale zanim je zatwierdzi, połączenie kończy się błędem. Tomek uruchamia `diagnose debug application fnbamd -1` i widzi, że `fw01` przestaje czekać na odpowiedź serwera RADIUS po kilku sekundach, bo timeout w `config user radius` jest domyślny. Po ustawieniu `timeout 60`, jak zaleca Microsoft dla rozszerzenia NPS z MFA, Kasia ma czas na zatwierdzenie i tunel wstaje.

Jak to działa

Pojęcie: dial-up i mode-cfg. W tunelu dial-up brama czeka na dowolnego klienta i dopiero po uwierzytelnieniu przydziela mu parametry: adres z puli, serwery DNS i listę sieci do tunelowania. Ten przydział nazywa się mode-cfg (mode configuration) i dzięki niemu klient nie musi znać z góry adresów w sieci Zielonej.



Rysunek 1. Dwie drogi pracownika do fw01: FortiClient albo wbudowany klient Windows trafiają do jednego tunelu dial-up, a uwierzytelnienie sprawdza NPS na dc02, grupy do zasobów daje FSSO z dc01. (kliknięcie otwiera pełny rozmiar)

Oba klienty łączą się z tym samym tunelem `vpn_zielona_user`, więc jedna konfiguracja na `fw01` obsługuje obie drogi. Różnią się tylko tym, co leży po stronie laptopa: profil ProfileXML wgrany przez RMM albo Intune, albo program FortiClient z własnym połączeniem. Certyfikat bramy musi mieć dobre EKU i SAN w obu przypadkach, jak opisuje strona Błąd 13801.

IKEv2 z EAP działa w dwóch krokach. Brama dowodzi tożsamości certyfikatem serwera, a użytkownik dowodzi swojej tożsamości metodą EAP (hasło albo certyfikat użytkownika), którą `fw01` przekazuje do serwera RADIUS. Tabelę metod uwierzytelniania i ograniczenia profilu Windows opisuje strona o pojęciach, a tu przyjmujemy, że wybór metody już zapadł.

Formy FortiClient

FortiClient występuje w kilku formach i tylko informacyjnie je tu zestawiamy. Warunki licencji i dostępne wersje sprawdzamy u dystrybutora i w dokumentacji, bo Fortinet je w ostatnich latach zmieniał.

Forma	Co oferuje	Uwagi
FortiClient VPN-only (bezpłatny)	podstawowy IPsec i SSL VPN z kluczem PSK albo certyfikatem, split tunnel, FortiToken, bez centralnego zarządzania, autoconnect, VPN przed logowaniem i wsparcia producenta [5]	wersja dla Windows zamrożona na 7.4.3, wydania 7.4.4 do 8.0.0 nie mają nowej wersji tego agenta, a poprawki bezpieczeństwa dla 7.4.3 przychodzą osobno [6]
FortiClient z licencją i EMS	zarządzanie centralne, autoconnect, VPN przed logowaniem, ZTNA, sprawdzanie stanu urządzenia	licencja na urządzenie w FortiClient EMS, EMS ma modele bezpłatny i płatne [7]
FortiClient Standalone z FortiIdentity Cloud	nowa pozycja w dokumentacji FortiOS 8.0	opis i licencję sprawdzamy w dokumentacji, nie opisujemy ich tu [8]

Od wersji 7.4.4 FortiClient nie obsługuje IKEv1 w IPsec, więc tunel dial-up musi używać IKEv2, jak w tej książce [9]. Funkcja IPsec przez TCP (port 443) działa w FortiClient 7.4.3 i nowszych na Windows i macOS tylko w wersji licencjonowanej [10]. FortiClient dla Linuksa według Fortinet Community nie obsługuje IPsec, więc na Linuksie używamy innego klienta IKEv2, na przykład strongSwan [11].

Split tunnel a pełny tunel

Zasięg tunelu ustawiamy na `fw01` i on decyduje, co laptop wyśle do firmy.

Cecha	Split tunnel	Pełny tunel
Co idzie przez `fw01`	tylko ruch do sieci z `ipv4-split-include`	cały ruch klienta, także do stron internetowych
Obciążenie łącza i zapory	małe	duże, całe przeglądanie przechodzi przez łącze biura
Kontrola i dziennik	ruch do firmy	całość, można stosować filtr WWW
Klient Windows	trasy trzeba mieć w ProfileXML, bo wbudowany klient ignoruje trasy przysłane przez bramę (strona o AlwaysOn)	wystarczy `RoutingPolicyType` ForceTunnel w profilu
Typowe zastosowanie	handlowcy z Optimą i WMS	osoby pracujące w nieufnych sieciach, audyt

W Zielonej pozostajemy przy split tunnelu, jak na stronie AlwaysOn VPN. Pełny tunel wymaga dodatkowej polityki z tunelu do `wan1` z NAT, a przy awarii `wan1` cały internet pracownika znika razem z tunelem.

```
config firewall policy
    edit 0
        set name "VPN-Zielona-do-internetu"
        set srcintf "vpn_zielona_user"
        set dstintf "wan1"
        set srcaddr "VPN_PULA"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

Polityka ze strony o EAP-TLS ma ustawione `nat enable` także dla ruchu do LAN, co sprawia, że serwery widzą adres `fw01`, a nie adres pracownika z puli 10.20.200.0/24. Dla logów i reguł opartych na adresie wolimy `nat disable` w polityce `VPN-Zielona-do-LAN`, a trasa powrotna do puli istnieje już na `fw01`. Tę różnicę zgłaszamy autorowi do decyzji.

Uwierzytelnianie przez RADIUS i NPS na dc02

NPS na `dc02` ma dwie role: sprawdza użytkownika w Active Directory i decyduje, czy wolno mu otworzyć tunel. Zasadę sieciową tworzymy w konsoli NPS, a nie przez PowerShell, bo kreator pilnuje kolejności warunków i metod.

```
Network Policy Server → Policies → Network Policies → New
Conditions: Windows Groups = ZIELONA\GG_VPN_Uzytkownicy
Conditions: Client Friendly Name = fw01
Constraints → Authentication Methods: PEAP z MS-CHAPv2 albo Smart Card or other certificate
(EAP-TLS)
```

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Network Policy Server z zasadą dla `fw01`, widoczne warunki Windows Groups z `GG_VPN_Uzytkownicy` i Client Friendly Name `fw01` oraz zaznaczone metody uwierzytelniania.

Metodę w zasadzie dobieramy do tunelu: EAP-TLS dla certyfikatu użytkownika według strony o EAP-TLS, PEAP z MS-CHAPv2 dla hasła i dla rozszerzenia MFA z następnej sekcji. NPS jest pojedynczym punktem awarii VPN, dlatego drugi NPS na `dc01` i `secondary-server` w `config user radius` rozważamy razem z planem wysokiej dostępności.

Drugi składnik logowania

Uwierzytelnianie hasłem to jeden składnik, więc przy audycie pana Wojtka pada pytanie o drugi. Mamy trzy drogi i żadna nie łączy się z każdą metodą EAP.

Droga	Jak działa	Ograniczenia
EAP-TLS z certyfikatem użytkownika	certyfikat z autorejestracji zastępuje hasło, klucz leży w TPM laptopa	to czynnik posiadania, bez kodu lub potwierdzenia, czy audytor uzna go za drugi składnik, ustalamy z panem Wojtkiem
Rozszerzenie NPS dla Microsoft Entra MFA	NPS po sprawdzeniu hasła prosi Microsoft Entra o potwierdzenie w aplikacji lub telefon	działa z PEAP z MS-CHAPv2, nie z EAP-TLS, wymaga synchronizacji z Entra ID i licencji z Microsoft Entra ID P1 albo P2, rozszerzenie instalujemy na serwerze NPS, nie na bramie VPN [2][12]
Token na FortiGate	FortiToken Mobile albo FortiIdentity Cloud, kod wpisywany w kliencie	wymaga licencji, FortiClient pokazuje pole na kod, wbudowany klient Windows nie obsługuje takiego pola (do sprawdzenia w naszej wersji)

Microsoft zaznacza, że kod TOTP w rozszerzeniu NPS nie działa z niektórymi klientami, w tym z wbudowanym klientem VPN Windows, więc w profilu AlwaysOn pozostaje potwierdzenie przez aplikację [2]. Fortinet opisuje także wariant „2FA” dla IKEv2, w którym tunel sprawdza jednocześnie certyfikat klienta i hasło przez EAP (`peertype peer` razem z `eap enable`), co wymaga FortiClient [13]. Wbudowany profil Windows wybiera jedną metodę, jak opisuje strona o pojęciach IPsec.

FortiClient a wbudowany klient Windows

Cecha	FortiClient	Wbudowany klient Windows (AlwaysOn)
Koszt	wersja bezpłatna zamrożona, nowsze wersje z licencją	brak

Cecha	FortiClient	Wbudowany klient Windows (AlwaysOn)
Instalacja	program na każdym laptopie	profil ProfileXML przez RMM albo Intune, tunel łączy się sam
Trasy split tunnel	pobiera z `fw01`	zapisane w profilu, bo trasy z bramy są ignorowane
Tunel automatyczny i przed logowaniem	tylko wersja z licencją	tunel użytkownika automatyczny, tunel urządzenia wymaga Windows 11 Enterprise lub Education
Metody EAP	PSK, certyfikat, EAP, certyfikat razem z EAP	jedna metoda w profilu: EAP-TLS lub PEAP
Kod z tokena	tak	nie
IPsec przez TCP 443	tak, wersja z licencją	nie
Stan urządzenia i ZTNA	z EMS, patrz SSL VPN i ZTNA	zgodność z Intune, patrz zgodność i dostęp warunkowy
Systemy	Windows, macOS, mobilne, Linux bez IPsec	tylko Windows

Dla laptopów Zielonej z Windows 11 proponujemy zostać przy wbudowanym kliencie z AlwaysOn, bo nie kosztuje i działa bez interakcji. FortiClient dokładamy, gdy potrzebujemy IPsec przez TCP 443, kodu z tokena, ZTNA albo klienta na macOS i telefonie. Przy awarii łącza głównego klient musi wskazać drugą bramę: wbudowany klient przez zmianę rekordu DNS, jak na stronie Łącza operatora, FortiClient według dokumentacji także przez listę bram (sprawdzamy w naszej wersji). Co ta brama oznacza przy zmiennym adresie Starlinka, opisuje następna sekcja.

Drugie łącze i adres bramy

Tunel dial-up z tej strony słucha na interfejsie ustawionym w `phase1-interface`, więc dla `wan2` potrzebujemy osobnej definicji tunelu albo wariantu opisanego w dokumentacji naszej wersji FortiOS.

Przy adresie, który może się zmienić, mamy dwie drogi dla pracowników. Pierwsza to dynamiczny DNS: `fw01` zgłasza adres `wan2` do FortiGuard DDNS albo własnej strefy, a rekord `vpn` w awarii wskazuje tę nazwę, co działa po upływie TTL. Druga to punkt zaczepienia w chmurze: `edge-az01` ze stałym adresem przekazuje UDP 500 i 4500 tunelem do `fw01`, a klienci dalej używają tej samej nazwy. Drugą drogę traktujemy jako wariant do próby w laboratorium, bo zachowanie NAT-T przy przekierowaniu docelowym i wiązanie tunelu z interfejsem loopback musimy potwierdzić na naszej wersji.

Certyfikat bramy zostaje ten sam w obu drogach, bo klient sprawdza nazwę z profilu, a nie adres, więc SAN `vpn.zielona.example` pasuje, o czym przypomina strona Błąd 13801. Klient Windows używa jednej nazwy z profilu, więc przełączenie robimy zmianą rekordu, a nie drugą bramą w profilu (zachowanie klienta przy kilku adresach sprawdzamy w teście).

Częste błędy

Objaw	Przyczyna	Co robimy
Użytkownik dostaje powiadomienie MFA, ale tunel odpada	timeout RADIUS na `fw01` krótszy niż czas na potwierdzenie	ustawiamy `timeout 60` albo więcej w `config user radius` [2]
`diagnose test authserver radius` zwraca odrzucenie, choć hasło jest dobre	zły wspólny sekret, `fw01` nie jest klientem RADIUS w NPS albo zasada NPS nie pasuje	sprawdzamy `New-NpsRadiusClient`, sekret i warunki zasady, a w dzienniku NPS powód odrzucenia
Klient łączy się, ale nie widzi `sql01` ani `fs01`	brak trasy do sieci w profilu Windows albo pusty `ipv4-split-include`	w ProfileXML dopisujemy trasy, na `fw01` sprawdzamy `ZIELONA_SIEC`
Nazwy `.ad.zielona.example` się nie rozwiązują	brak serwerów DNS w mode-cfg albo brak `DomainNameInformation` w profilu	ustawiamy `dns-mode manual` z `dc01` i `dc02`, w profilu dopisujemy NRPT
FortiClient nie łączy po aktualizacji do 7.4.4 lub nowszej	tunel używa IKEv1	przestawiamy tunel na `ike-version 2` [9]
IPsec przez TCP nie działa w bezpłatnym FortiClient	funkcja jest tylko w wersji licencjonowanej od 7.4.3	planujemy licencję albo zostajemy przy UDP 500 i 4500 [10]
Serwery widzą w logach tylko adres `fw01` zamiast adresu pracownika	w polityce VPN do LAN jest `nat enable`	ustawiamy `nat disable` po sprawdzeniu trasy powrotnej
Po awarii NPS nikt nie loguje się do VPN	jedna instancja NPS na `dc02`	dokładamy drugi NPS i `secondary-server` w `config user radius`
Po przełączeniu na Starlink klient VPN nie łączy się, choć internet działa	rekord `vpn` nadal wskazuje 203.0.113.10 albo stary adres `wan2`, który się zmienił	odczytujemy aktualny adres `wan2`, sprawdzamy aktualizację DDNS i zmieniamy rekord albo przechodzimy na punkt zaczepienia w chmurze

□□ Ćwiczenia

1. Dlaczego rozszerzenie NPS dla Microsoft Entra MFA nie pasuje do uwierzytelniania EAP-TLS i co wybieramy, jeśli chcemy potwierdzenia w aplikacji?

Odpowiedź

Microsoft opisuje integrację NPS z VPN dla MS-CHAPv2 i PEAP, a inne metody EAP nie są obsługiwane. Jeśli chcemy potwierdzenia w aplikacji, zmieniamy metodę na PEAP z MS-CHAPv2 i dokładamy rozszerzenie NPS. Przy EAP-TLS drugim składnikiem jest sam certyfikat w TPM.

1. Pracownik używa wbudowanego klienta Windows i po połączeniu widzi tylko `dc01`, choć w `ZIELONA_SIEC` są trzy sieci. Co sprawdzamy w pierwszej kolejności?

Odpowiedź

Sekcję `Route` w ProfileXML, bo wbudowany klient ignoruje trasy przysłane przez FortiGate i bierze tylko te z profilu. Potem sprawdzamy, czy polityka na `fw01` dopuszcza ruch do pozostałych sieci.

1. Handlowiec chce użyć bezpłatnego FortiClient z IPsec przez TCP 443, bo hotel blokuje UDP. Co mu odpowiadamy?

Odpowiedź

IPsec przez TCP w FortiClient 7.4.3 i nowszych na Windows jest tylko w wersji licencjonowanej, więc w bezpłatnej wersji nie zadziała. Rozwiązaniem jest licencja FortiClient albo inna sieć, w której UDP 500 i 4500 przechodzą.

Powiązane: IPsec i IKEv2 po ludzku: fazy, propozycje, uwierzytelnianie, Błąd 13801: certyfikat bramy VPN, EKU i SAN, AlwaysOn VPN: tunel użytkownika z ProfileXML, EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD, IPsec site-to-site: Pamiątkowo i Swarzędz między FortiGate a routerem innej firmy, Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate, SSL VPN i ZTNA: co z SSL VPN w nowych FortiOS i czym go zastąpić, Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI

Źródła:

1. Fortinet Community, „Troubleshooting Tip: How to test FortiGate's radius user authentication to the RADIUS server”: community.fortinet.com
2. Microsoft Learn, „Integrate your existing NPS infrastructure with Microsoft Entra multifactor authentication” oraz „Integrate your Remote Desktop Gateway and VPN servers with NPS extension”: learn.microsoft.com, learn.microsoft.com
3. Microsoft Learn, „New-NpsRadiusClient (NPS)”: learn.microsoft.com
4. Fortinet Community, „Technical Tip: How to configure IPsec VPN tunnel using IKE v2”: community.fortinet.com

5. Fortinet Community, „Technical Tip: FortiClient licensing and support”: community.fortinet.com
6. Fortinet Document Library, „FortiClient 7.4.8 Windows Release Notes, Special notices” oraz Fortinet Community, „Is FortiClient 7.4.3 the last ever free version”: docs.fortinet.com, community.fortinet.com
7. Fortinet Document Library, „FortiClient feature comparison” (8.0.0): docs.fortinet.com
8. Fortinet Document Library, „VPN with FortiClient Standalone and FortiIdentity Cloud” (FortiOS 8.0.0): docs.fortinet.com
9. Fortinet Document Library, „FortiClient 7.4.8 Windows Release Notes, Special notices”: docs.fortinet.com
10. Fortinet Community, „Technical Tip: How to configure IPsec over TCP”: community.fortinet.com
11. Fortinet Community, „FortiClient VPN on Linux, IPsec remote access VPN not available (FortiOS 7.6.6)”: community.fortinet.com
12. Microsoft Learn, „Integrate your existing NPS infrastructure with Microsoft Entra multifactor authentication”: learn.microsoft.com
13. Fortinet Document Library, „IPsec IKEv2 VPN 2FA with EAP and certificate authentication”: docs.fortinet.com

---

Revision #11
Created 2026-10-03 19:10:57 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:20 UTC by Tomasz Konieczny