SSL VPN i ZTNA: co z SSL VPN w nowych FortiOS i czym go zastąpić

Poziom: zaawansowany

Dotyczy: FortiGate 100F (FortiOS 7.4, 7.6 i 8.0), FortiClient, FortiClient EMS (stan na październik 2026)

Czas: ~40 min

Fortinet usunął z FortiOS tryb tunelowy SSL VPN, więc zapory z nowszym oprogramowaniem muszą przejść na IPsec albo na dostęp do pojedynczych aplikacji (ZTNA). Strona pokazuje, od której wersji to obowiązuje, co dzieje się na `fw01` (FortiGate 100F), jak migrujemy i kiedy wybieramy który sposób zdalnego dostępu. Wracamy tu przed każdą aktualizacją FortiOS i przy każdym pytaniu o dostęp dla firmy zewnętrznej.

ZAŁOŻENIA SCENARIUSZA

migrację opisujemy dla pojedynczego `fw01` z jednym łączem (`wan1`, 203.0.113.10), na którym kończą się wszystkie VPN. W parze FortiGate konfiguracja jest wspólna dla obu sztuk, a aktualizacje robimy według strony Para FortiGate w klastrze: FGCP aktywny-pasywny.

Skróty użyte na tej stronie (18)

Skrót	Co znaczy
ADVPN	Auto-Discovery VPN: funkcja FortiGate, w której oddziały same zestawiają tunele między sobą bez ruchu przez centralę
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
EMS	FortiClient Enterprise Management Server: serwer Fortinet, który zarządza klientami FortiClient, zbiera stan urządzeń i nadaje tagi dla ZTNA
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
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

Skrót	Co znaczy
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
JWT	JSON Web Token: podpisany token z danymi, tu przenoszący tagi stanu urządzenia z FortiClient do FortiOS
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
RDP	Remote Desktop Protocol: protokół pulpitu zdalnego Windows, uruchamiany poleceniem mstsc
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TFAP	TCP Forwarding Access Proxy: tryb ZTNA na FortiGate, który przekazuje do aplikacji zwykłe połączenia TCP, na przykład RDP
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
UDP	User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem
ZTNA	Zero Trust Network Access: dostęp do pojedynczych aplikacji po sprawdzeniu użytkownika i stanu jego urządzenia, bez wpuszczania do całej sieci

Fiszka

Komendy wykonujemy w CLI `fw01`, wszystkie poza ostatnią tylko czytają.

□□ TYLKO ODCZYT

Sprawdzenie wersji i modelu: get system status

```
get system status
```

Wypisuje model, wersję FortiOS, numer seryjny i stan licencji. Wersję porównujemy z tabelą niżej, zanim zaplanujemy aktualizację.

Przykład (skrócony, poglądowy):

```
Version: FortiGate-100F v7.4.x,buildNNNN,(GA.M)
Hostname: fw01
Operation Mode: NAT
```

□□ **get** = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

□□ TYLKO ODCZYT

Sprawdzenie ustawień SSL VPN: show vpn ssl settings

```
show vpn ssl settings
```

Pokazuje, czy SSL VPN w ogóle jest skonfigurowany: interfejs źródłowy, port, pule adresów trybu tunelowego i reguły uwierzytelniania. Pusty wynik oznacza, że nie mamy czego migrować.

□□ **SSL** = Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

□□ TYLKO ODCZYT

Sprawdzenie zalogowanych użytkowników SSL VPN: get vpn ssl monitor

```
get vpn ssl monitor
```

Wypisuje bieżące sesje SSL VPN z nazwą użytkownika i adresem, z którego się łączy. Jeśli po tygodniu obserwacji lista jest pusta, wiemy, że wyłączenie niczego nie zepsuje.

□□ **SSL** = Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **get** = FortiOS: polecenia odczytu stanu urządzenia, na przykład get system status pokazuje wersję i numer seryjny

□□ TYLKO ODCZYT

Znalezienie polityk z interfejsem SSL VPN: show firewall policy | grep -f ssl.root

```
show firewall policy | grep -f ssl.root
```

Wypisuje polityki, które odwołują się do interfejsu `ssl.root`. Fortinet pisze, że takie polityki trzeba po migracji odtworzyć na interfejsie tunelu IPsec, więc ich liczba mówi, ile pracy nas czeka [1].

SSL = Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS · **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 · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

ZMIENIA SYSTEM

Przejście na IPsec przez TCP 443: config system settings

```
config system settings
    set ike-tcp-port 443
end
config vpn ipsec phase1-interface
    edit "vpn_zielona_user"
        set transport tcp
    next
end
```

Włącza transport TCP dla tunelu dial-up, żeby klienci w sieciach blokujących UDP 500 i 4500 mogli łączyć się tym samym portem, którego używał SSL VPN. Funkcja działa tylko z IKEv2, nie obsługuje ADVPN i wymaga FortiClient w wersji licencjonowanej [2]. Przed ustawieniem 443 sprawdzamy, czy port nie jest zajęty przez Agentless VPN albo panel administracyjny na tym samym interfejsie.

IPsec = Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2 · **TCP** = Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia · **UDP** = User Datagram Protocol: szybki protokół sieciowy bez potwierdzeń · **SSL** = Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **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 · **ADVPN** = Auto-Discovery VPN: funkcja FortiGate, w której oddziały same zestawiają tunele między sobą bez ruchu przez centralę

Z życia wzięte

Z ŻYCIA WZIĘTE

Wtorek, 11:00. Tomek przygotowuje aktualizację `fw01` z gałęzi 7.4 do 7.6 i na wszelki wypadek sprawdza `show vpn ssl settings`. Okazuje się, że przed laty firma serwisująca WMS dostała dostęp przez przeglądarkę, a w konfiguracji została pula adresów trybu tunelowego, o której nikt nie pamiętał. Przed aktualizacją Tomek ustala z Markiem, czy ta firma jeszcze pracuje, i zamiast portalu SSL planuje dla niej dostęp do jednej aplikacji.

Co dokładnie zniknęło

> **Pojęcie: tryb tunelowy i tryb webowy.** Tryb tunelowy SSL VPN buduje z klientem (FortiClient) tunel przez połączenie TLS, który obejmuje cały ruch albo wybrane sieci, podobnie jak IPsec. Tryb webowy to portal w przeglądarce z listą aplikacji (strony, SSH, RDP), bez instalowania klienta.

Od FortiOS 7.6.3 (2025) tryb tunelowy SSL VPN jest zastąpiony przez IPsec i dotyczy to wszystkich modeli FortiGate [1]. Tryb webowy zostaje pod nową nazwą Agentless VPN. Konfiguracja trybu tunelowego nie jest przenoszona podczas aktualizacji do 7.6.3, więc migrujemy ją przed aktualizacją, a nie po niej [1].

Wersja FortiOS	Tryb tunelowy SSL VPN	Tryb webowy (Agentless VPN)
7.4.x	jest	jest
7.6.0 do 7.6.2	jest na FortiGate 100F i nowszych modelach serii F, nie ma na 40F i 60F	jest
7.6.3 i nowsze	nie ma na żadnym modelu	jest, ale nie na modelach 40F, 60F i 90G, a 100F nie jest wymieniony wśród wyjątków (sprawdzamy w notatkach wydania naszej wersji) [3]
8.0.0	w liście nowości 8.0.0 nie znaleźliśmy SSL VPN, pojawiają się za to IPsec przez TLS 1.3 i uproszczenia ZTNA [4]	do sprawdzenia w notatkach wydania

Dla FortiGate 100F oznacza to, że tryb tunelowy działa do 7.6.2 włącznie, a od 7.6.3 nie ma go wcale. Fortinet Community dopuszcza pozostanie na 7.6.2 lub starszej, ale wtedy rezygnujemy z późniejszych poprawek, czyli zostawiamy na zewnątrz komponent, z którym wiązały się podatności [5]. Wersję `fw01` zapisujemy w NetBoxie po sprawdzeniu `get system status`, bo w bazie jest dziś tylko ogólny zapis 7.4/7.6.

FortiClient jako klient SSL VPN dla nowych FortiOS jest wycofany i Fortinet wskazuje dial-up IPsec jako zamiennik [1]. Tego, jak wygląda ten tunel po stronie `fw01` i klienta, uczy strona IPsec dla

pracowników: FortiClient i dial-up IKEv2 na FortiGate.

Migracja z SSL VPN do IPsec

Fortinet opisuje migrację w krokach: kopia konfiguracji, przeniesienie ustawień na `fw01` i w FortiClient (w interfejsie, w CLI albo usługą FortiConverter), równoległa praca obu rozwiązań, test, aktualizacja i na końcu wyłączenie SSL VPN w EMS [1]. Wymagania wersji to FortiOS 7.4.2 lub nowszy dla transportu TCP i FortiClient 7.4.1 lub nowszy dla IPsec przez TCP, a przy zarządzaniu przez FortiManager najpierw aktualizujemy FortiManager [1].

Element SSL VPN	Odpowiednik w IPsec
pula adresów trybu tunelowego	pula mode-cfg `ipv4-start-ip` i `ipv4-end-ip`
routing tunelowania wybranych sieci	`ipv4-split-include`
grupy w regułach uwierzytelniania	`authusrgrp` w tunelu albo grupy w polityce
interfejs `ssl.root` w politykach	interfejs tunelu IPsec, na przykład `vpn_zielona_user`
port 443	`transport tcp` i `ike-tcp-port` (UDP 500 i 4500 domyślnie)
FortiClient z SSL VPN	FortiClient z IPsec IKEv2 albo wbudowany klient Windows

W Zielonej pracownicy łączą się już przez IPsec IKEv2, więc ta migracja obejmuje tylko ewentualne konfiguracje historyczne, jak w scence. Dla firmy zewnętrznej, której trzeba dać dostęp tylko do jednej aplikacji, rozważamy Agentless VPN albo ZTNA zamiast pełnego tunelu.

Znane podatności jako uzasadnienie

Nie znaleźliśmy w dokumentacji Fortinet jednego zdania uzasadniającego usunięcie trybu tunelowego. Komentatorzy branżowi wiążą decyzję z serią krytycznych błędów w usłudze obsługującej SSL VPN [6]. Poniższe trzy pozycje pokazują wzór, bez szczegółów, które pomagałyby w ataku.

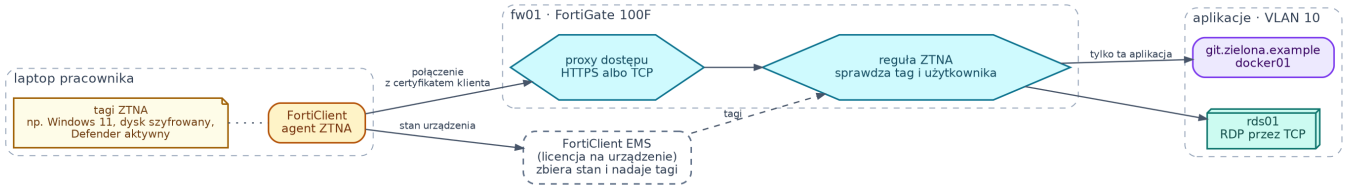
Oznaczenie	Rok	Rodzaj błędu	Stan według źródeł
CVE-2022-42475	2022	przepełnienie bufora na stercie w procesie SSL VPN, wykonanie kodu bez logowania	wykorzystywany w atakach [7]

Oznaczenie	Rok	Rodzaj błędu	Stan według źródeł
CVE-2023-27997	2023	przepełnienie bufora na stercie w SSL VPN, wykonanie kodu przed uwierzytelnieniem	wykorzystywany w atakach, MFA nie chroni, bo błąd leży przed logowaniem [8]
CVE-2024-21762	2024	zapis poza zakresem pamięci w procesie SSL VPN, wykonanie kodu bez logowania	wykorzystywany w atakach, potwierdzone przez CISA [9]

Wniosek dla projektu jest praktyczny. Usługa SSL VPN nasłuchuje na adresie publicznym i obsługuje żądania, zanim ktokolwiek się zaloguje, więc błąd w niej daje atakującemu dostęp do zapory bez konta. Czy tryb webowy dzieli ten sam kod i te same ryzyka, w dostępnych źródłach nie znaleźliśmy jednoznacznie, więc traktujemy Agentless VPN jako wystawioną powierzchnię ataku i włączamy go tylko tam, gdzie jest uzasadniony.

ZTNA: dostęp do aplikacji, nie do sieci

> **Pojęcie: ZTNA.** Zero Trust Network Access to dostęp do pojedynczej aplikacji po sprawdzeniu użytkownika i stanu jego urządzenia, bez wpuszczania go do całej sieci. Zamiast tunelu do sieci 10.20.10.0/24 pracownik dostaje drogę do jednego adresu, na przykład `git.zielona.example`, i tylko dopóki jego laptop spełnia warunki.



Rysunek 1. ZTNA w Zielonej: FortiClient zgłasza stan laptopa do EMS, EMS nadaje tagi, a fw01 jako proxy dostępu wpuszcza do git.zielona.example i rds01 tylko urządzenia z odpowiednimi tagami. (kliknięcie otwiera pełny rozmiar)

Elementy układu to proxy dostępu na `fw01` (serwer ZTNA), reguły ZTNA, FortiClient na laptopie, FortiClient EMS i certyfikaty. Reguła sprawdza tag, czyli etykietę stanu urządzenia nadaną przez EMS na podstawie danych z FortiClient, na przykład czy działa antywirus, czy zapora jest włączona i czy poprawki są aktualne [10]. W FortiOS 8.0 FortiClient potrafi też przesyłać tagi do FortiOS

bezpośrednio w tokenie JWT [4]. Dostęp ma dwie formy: proxy HTTPS dla aplikacji webowych i proxy TCP (TFAP) dla innych usług, na przykład RDP do `rds01` [11].

Forma licencji jest prosta do opisania i trudna do ominięcia. Według Fortinet Community sama zapora nie wymaga osobnej licencji ZTNA, a licencje kupujemy w EMS na liczbę urządzeń, czyli na każdy laptop korzystający z ZTNA [12]. Dokładny rodzaj i cenę sprawdzamy u dystrybutora, bo Fortinet zmieniał nazwy pakietów, a pan Zbigniew zapyta o koszt przed pierwszym szkoleniem.

Wdrożenie przebiega w kilku krokach, których składnię opisuje dokumentacja „Basic ZTNA configuration” [10]: połączenie `fw01` z EMS, definicja tagów, certyfikat dla proxy dostępu, serwer ZTNA z adresem publicznym, reguła z tagami i na końcu polityka. Dla Zielonej proponujemy pilotaż z jedną aplikacją, `git.zielona.example` na `docker01`, i grupą programistów Oli, a RDP do `rds01` dokładamy po teście.

Kiedy który

Potrzeba	Wybór	Dlaczego
Pracownik potrzebuje całej sieci Zielonej (Optima, WMS, udziały)	IPsec dial-up IKEv2	standard, wbudowany klient Windows, jeden tunel na wiele aplikacji
Laptop bywa w sieci blokującej UDP	IPsec przez TCP 443 z licencjonowanym FortiClient	ten sam port co dawny SSL VPN
Firma zewnętrzna potrzebuje jednej strony lub RDP, a my nie chcemy jej wpuszczać do sieci	ZTNA, ewentualnie Agentless VPN	dostęp tylko do wskazanej aplikacji, bez klienta w przypadku portalu
Zależy nam na sprawdzaniu stanu urządzenia przy każdym połączeniu	ZTNA z EMS	tagi decydują o dostępie, nie samo hasło
Administrator potrzebuje szybkiego tunelu do laboratorium i VLAN 98	WireGuard na Linuksie	patrz WireGuard i OpenVPN, FortiOS go nie obsługuje

Częste błędy

Objaw	Przyczyna	Co robimy
Po aktualizacji do 7.6.3 nie ma konfiguracji trybu tunelowego	Fortinet nie przenosi jej przy aktualizacji	przed aktualizacją migrujemy do IPsec i zachowujemy kopię konfiguracji [1]
Polityki z `ssl.root` znikają albo przestają działać	interfejs `ssl.root` nie istnieje w nowszych wersjach	odtwarzamy polityki na interfejsie tunelu IPsec [1]

Objaw	Przyczyna	Co robimy
Po migracji klienci nadal próbują łączyć się przez SSL VPN	FortiClient ma stary profil z SSL VPN	wysyłamy nowy profil IPsec i wyłączamy SSL VPN w EMS po teście [1]
IPsec przez TCP 443 nie startuje	port zajęty, wersja FortiOS lub FortiClient za stara, brak licencji klienta	sprawdzamy wersje i licencję, a port ustawiamy w `ike-tcp-port` [2]
Wyłączyliśmy SSL VPN, a firma zewnętrzna nie ma dostępu	nikt nie sprawdził, kto korzysta z portalu	przed wyłączeniem czytamy `get vpn ssl monitor` przez tydzień i pytamy właściciela dostępu
ZTNA odrzuca prawidłowego użytkownika	laptop nie ma wymaganego tagu albo EMS go jeszcze nie zsynchronizował	sprawdzamy tagi na `fw01` i w EMS, czekamy na synchronizację [10]

□□ Ćwiczenia

1. `fw01` pracuje na FortiOS 7.6.2 z pulą adresów trybu tunelowego SSL VPN. Co robimy przed aktualizacją do 7.6.4?

Odpowiedź

Najpierw kopia konfiguracji i sprawdzenie, kto używa SSL VPN (`get vpn ssl monitor`). Potem konfigurujemy równolegle tunel IPsec dial-up (pula, split tunnel, grupy, polityka na interfejsie tunelu) i testujemy go z FortiClient. Dopiero po teście aktualizujemy, bo od 7.6.3 konfiguracja trybu tunelowego nie jest przenoszona.

1. Czym różni się dostęp ZTNA od IPsec dial-up z punktu widzenia tego, co laptop pracownika widzi w sieci?

Odpowiedź

W IPsec dial-up laptop dostaje adres z puli i dostęp do wskazanych sieci, na przykład całej 10.20.10.0/24. W ZTNA laptop widzi tylko opublikowane aplikacje, na przykład `git.zielona.example`, a reguła sprawdza przed każdym połączeniem tag stanu urządzenia.

1. Dlaczego włączenie MFA nie obroniłoby przed błędem takim jak CVE-2023-27997?

Odpowiedź

Bo błąd leży w obsłudze żądań przed uwierzytelnieniem, więc atakujący nie dochodzi do etapu logowania, na którym działałby drugi składnik. Obroną jest aktualizacja, ograniczenie ekspozycji i rezygnacja z usługi, której nie potrzebujemy.

Powiązane: VPN: tunel przez cudzy internet, IPsec i IKEv2 po ludzku: fazy, propozycje, uwierzytelnianie, IPsec dla pracowników: FortiClient i dial-up IKEv2 na FortiGate, WireGuard i OpenVPN: odpowiedniki spoza FortiGate na Linuksie, Zgodność i dostęp warunkowy w Intune

Źródła:

1. Fortinet Document Library, „SSL VPN tunnel mode to IPsec VPN migration” (FortiOS 7.6.3) oraz „SSL VPN tunnel mode no longer supported” (Release Notes 7.6.3): docs.fortinet.com , docs.fortinet.com
2. Fortinet Community, „Technical Tip: How to configure IPsec over TCP”: community.fortinet.com
3. Fortinet Community, „Technical Tip: SSL VPN support on FortiGate models”: community.fortinet.com
4. Fortinet Document Library, „FortiOS 8.0.0 New Features”: docs.fortinet.com
5. Fortinet Community, „SSL-VPN Tunnel Mode Support with FortiClient in FortiOS 7.6.3 and Beyond”: community.fortinet.com
6. IT-Connect, „Fortinet annonce la fin du support du VPN SSL dans FortiOS 7.6.3”: it-connect.fr
7. CIRCL, „TR-71: FortiOS heap-based buffer overflow in sslvpnd (CVE-2022-42475)”: circl.lu
8. The Stack, „Fortinet vulnerability VPN (CVE-2023-27997)”: thestack.technology
9. Rapid7, „Critical Fortinet FortiOS CVE-2024-21762 exploited”: rapid7.com
10. Fortinet Document Library, „Basic ZTNA configuration” (FortiOS 7.6.4): docs.fortinet.com
11. Fortinet Document Library, „FortiClient feature comparison” (8.0.0): docs.fortinet.com
12. Fortinet Community, „Fortinet ZTNA licensing”: community.fortinet.com

---

Revision #11
Created 2026-10-03 19:10:58 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:22 UTC by Tomasz Konieczny