Błąd 13801: certyfikat bramy VPN, EKU i SAN

Poziom: średni

Dotyczy: AD CS (Windows Server 2019/2022), FortiGate 100F (FortiOS 7.4/7.6), Windows 11

Czas: ~30 min

Windows odrzuca certyfikat bramy VPN z kodem 13801 albo 13806 częściej z powodu złego pola w certyfikacie niż z powodu samego hasła. Ta strona pokazuje, co dokładnie sprawdza klient, jak wystawić poprawny certyfikat z AD CS i jak to zweryfikować, zanim zadzwoni pierwsza osoba z terenu.

ZAŁOŻENIA SCENARIUSZA

certyfikat bramy VPN instalujemy na pojedynczym `fw01` w centrali, pod adresem `vpn.zielona.example` (203.0.113.10, jedno łącze `wan1`). Urząd certyfikacji AD CS stoi na `dc01` w VLAN 10. W parze FortiGate konfigurację bramy synchronizuje klaster: Para FortiGate w klastrze: FGCP aktywny-pasywny.

Skróty użyte na tej stronie (16)

Skrót	Co znaczy
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
CN	Common Name: główna nazwa w certyfikacie, np. adres serwera
CRL	Certificate Revocation List: lista certyfikatów unieważnionych przed upływem ich terminu ważności
EKU	Extended Key Usage: pole w certyfikacie mówiące, do czego wolno go używać, na przykład wyłącznie do uwierzytelniania serwera
GUI	Graphical User Interface: okienka i myszka zamiast komend
IKE	Internet Key Exchange: protokół, który przed popłynięciem danych dogaduje między dwiema stronami klucze i reguły szyfrowania tunelu IPsec

Skrót	Co znaczy
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)
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
NetBIOS	Network Basic Input/Output System: stara warstwa nazw w sieciach Windows; nazwa komputera w niej ma najwyżej 15 znaków, co ogranicza długość nazwy punktu dostępu klastra
PKCS	Public Key Cryptography Standards: rodzina standardów kryptograficznych, tu chodzi o profil certyfikatu importowanego razem z gotowym kluczem prywatnym
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
TFTP	Trivial File Transfer Protocol: bardzo prosty protokół przesyłania plików bez uwierzytelniania, w FortiGate jedna z dróg wysłania kopii konfiguracji
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

□□ TYLKO ODCZYT

Sprawdzenie EKU i SAN wystawionego certyfikatu: certutil -dump

```
certutil -dump NazwaCertyfikatu.cer
```

Wypisuje pełną zawartość certyfikatu, w tym pole Enhanced Key Usage (EKU) i Subject Alternative Name (SAN). Uruchamiamy to polecenie na dowolnym pliku `.cer` czy `.crt`, zanim zaimportujemy go na bramę VPN, żeby złapać błąd przed wdrożeniem, a nie po telefonie od Kasi.

Przykład:

```
Podmiot CN=vpn.zielona.example, DC=ad, DC=zielona, DC=example
    ...
Rozszerzenie: Enhanced Key Usage
    Server Authentication (1.3.6.1.5.5.7.3.1)
Rozszerzenie: Subject Alternative Name
```

```
    DNS Name=vpn.zielona.example
```

EKU = Extended Key Usage: pole w certyfikacie mówiące, do czego wolno go używać, na przykład wyłącznie do uwierzytelniania serwera · **SAN** = w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa · **VPN** = Virtual Private Network: szyfrowany tunel do sieci firmowej · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

TYLKO ODCZYT

Sprawdzenie łańcucha zaufania i listy unieważnień: certutil -verify

```
certutil -verify -urlfetch NazwaCertyfikatu.cer
```

Sprawdza, czy certyfikat da się zweryfikować aż do zaufanego głównego urzędu certyfikacji, oraz czy jego lista unieważnień (CRL) jest aktualna i osiągalna. Flaga `-urlfetch` wymusza rzeczywiste pobranie CRL z adresu zapisanego w certyfikacie, zamiast polegać na lokalnym buforze.

Przykład:

```
Ścieżka certyfikatu zweryfikowana pomyślnie.
Sprawdzenie listy CRL: OK, ostatnia publikacja: 2026-09-20
```

CRL = Certificate Revocation List: lista certyfikatów unieważnionych przed upływem ich terminu ważności · **certutil** = narzędzie Windows do sprawdzania, importowania i eksportowania certyfikatów z linii poleceń

TYLKO ODCZYT

Import certyfikatu bramy na FortiGate przez TFTP: execute vpn certificate local import

```
execute vpn certificate local import tftp NazwaPliku.p12 AdresSerweraTftp p12 HasloPliku
```

Wgrywa na `fw01` certyfikat wraz z kluczem prywatnym z pliku PKCS#12 pobranego serwerem TFTP. Ten sam efekt osiągamy przez GUI (`System → Certificates → Import → Certificate`), ale wersja CLI nadaje się do automatyzacji wdrożenia albo odnowienia certyfikatu co roku.

TFTP = Trivial File Transfer Protocol: bardzo prosty protokół przesyłania plików bez uwierzytelniania, w FortiGate jedna z dróg wysłania kopii konfiguracji · **PKCS** = Public Key

Cryptography Standards: rodzina standardów kryptograficznych, tu chodzi o profil certyfikatu importowanego razem z gotowym kluczem prywatnym · **GUI** = Graphical User Interface: okienka i myszka zamiast komend · **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu · **execute** = FortiOS: polecenia, które coś wykonują na urządzeniu, na przykład execute backup config wysyła kopię konfiguracji, a execute ha manage otwiera sesję na drugiej zaporze w parze

Z życia wzięte

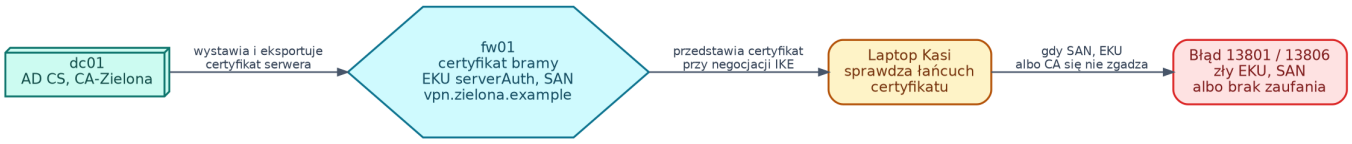
Z ŻYCIA WZIĘTE

Pan Zbigniew wraca z urlopu z nowym laptopem, który dział IT właśnie skonfigurował. Próbuje pierwszy raz połączyć się z VPN z domu i dostaje komunikat „Błąd 13801: poświadczenia uwierzytelniania IKE są niedopuszczalne". Dzwoni z pytaniem, czy to na pewno jego wina, bo hasło na pewno wpisał poprawnie.

Jak to działa

Rozwiń: jak to działa pod spodem

Podczas negocjacji fazy 1 brama `fw01` przedstawia klientowi swój certyfikat, zanim jeszcze klient poda cokolwiek o sobie. Wbudowany klient IKEv2 Windows sprawdza w tym certyfikacie trzy rzeczy niezależnie od siebie, i odrzucenie na którejkolwiek z nich kończy się błędem, mimo że hasło i konfiguracja tunelu po stronie użytkownika są całkowicie poprawne.



Droga certyfikatu bramy: dc01 wystawia, fw01 przedstawia klientowi, laptop sprawdza łańcuch zaufania (kliknięcie otwiera pełny rozmiar)

Pierwsza rzecz to pole **Enhanced Key Usage (EKU)**: certyfikat musi zawierać wpis Server Authentication (identyfikator `1.3.6.1.5.5.7.3.1`), bo to on mówi klientowi „ten certyfikat wolno używać do potwierdzania tożsamości serwera". Druga rzecz to pole **Subject Alternative**

Name (SAN): musi zawierać dokładnie tę nazwę, pod którą klient łączy się z bramą, w Zielonej `vpn.zielona.example`, a nie samą nazwę NetBIOS serwera ani adres IP. Trzecia rzecz to **łańcuch zaufania**: klient musi mieć w swoim magazynie zaufane certyfikaty urzędu, który podpisał certyfikat bramy, w Zielonej urzędu `CA-Zielona` z `dc01`, razem z aktualną listą CRL.

> **Pojęcie: szablon certyfikatu.** W AD CS gotowy zestaw ustawień, na podstawie którego wystawiane są certyfikaty tego samego typu. Certyfikat bramy VPN wystawiamy z szablonu `ZielonaWWW`: to kopia szablonu `Web Server` z EKU tylko Server Authentication, z nazwą podawaną w żądaniu (Supply in the request) i z zatwierdzeniem przez menedżera certyfikatów.

> Nazwę SAN podajemy w samym żądaniu jako rozszerzenie: w pliku `request.inf` dla `certreq` (sekcja `[Extensions]` z identyfikatorem `2.5.29.17` i wpisem `dns=vpn.zielona.example`) albo w pliku `san.cnf` dla OpenSSL, jak na stronie Generowanie certyfikatów: OpenSSL i urząd certyfikacji Windows. Szablon `ZielonaWWW` pozwala podać nazwę w żądaniu, więc urząd przepisuje SAN do certyfikatu bez żadnych zmian w swojej konfiguracji, a wniosek czeka na zatwierdzenie drugiej osoby z zespołu.

> ⚠ Starsze poradniki każą na czas wystawienia włączyć na urzędzie flagę `EDITF_ATTRIBUTESUBJECTALTNAME2` i podać SAN atrybutem `san:dns=...`. Tego nie robimy, nawet na chwilę: flaga to podatność ESC6, bo przez cały czas jej włączenia każdy, kto może poprosić o jakikolwiek certyfikat, dopisze w SAN nazwę konta administratora domeny. Jak sprawdzić, czy flaga nie została włączona dawniej, i jak ją wyłączyć na stałe, opisuje strona Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza.

Po wystawieniu certyfikatu z poprawnym EKU i SAN eksportujemy go razem z kluczem prywatnym do pliku PKCS#12 i wgrywamy na `fw01` fiszką wyżej. Weryfikację całości robimy dwuetapowo: `certutil -dump` na wyeksportowanym pliku, zanim trafi na bramę, i próbę połączenia z testowego laptopa, zanim wyślemy zmianę na całą flotę handlowców.

Częste błędy

Kod błędu	Znaczenie	Najczęstsza przyczyna
13801	IKE, poświadczenia uwierzytelniania są niedopuszczalne (ERROR_IPSEC_IKE_AUTH_FAIL)	certyfikat bramy bez EKU Server Authentication, SAN niezgodny z `vpn.zielona.example`, albo klient nie ufa urzędowi `CA-Zielona`
13806	IKE nie znalazło ważnego certyfikatu maszyny (ERROR_IPSEC_IKE_NO_CERT)	tunel skonfigurowany pod uwierzytelnienie certyfikatem, a na kliencie brak albo wygasł certyfikat maszyny czy użytkownika wymagany po tej stronie
809	połączenie sieciowe między komputerem a serwerem VPN nie mogło zostać nawiązane	port UDP 500 albo 4500 zablokowany po drodze, zwykle przez zaporę hotelową albo domową, nie problem samego IKE
812	połączenie odrzucone przez politykę serwera zdalnego dostępu	metoda uwierzytelniania w profilu klienta nie zgadza się z tym, czego oczekuje serwer, na przykład klient próbuje EAP-MSCHAPv2 tam, gdzie polityka wymaga uwierzytelnienia certyfikatem

□□ Ćwiczenia

1. Certyfikat bramy ma poprawny EKU Server Authentication, ale w polu SAN wpisano tylko nazwę NetBIOS `FW01`, bez pełnej nazwy `vpn.zielona.example`. Klient łączy się właśnie pod adresem `vpn.zielona.example`. Jaki błąd zobaczy i dlaczego?

Odpowiedź

Zobaczy błąd 13801. Windows porównuje nazwę, pod którą łączy się klient, z zawartością pola SAN certyfikatu, nie z jego polem Subject (CN) ani z samą nazwą NetBIOS. Skoro SAN nie zawiera `vpn.zielona.example`, certyfikat zostaje odrzucony, mimo poprawnego EKU i mimo zaufanego urzędu certyfikacji.

1. Tomek znalazł poradnik, według którego przed wystawieniem certyfikatu bramy trzeba na chwilę włączyć na urzędzie flagę `EDITF_ATTRIBUTESUBJECTALTNAME2`. Dlaczego tego nie robimy i jak dostajemy certyfikat z `vpn.zielona.example` w SAN?

Odpowiedź

Flaga pozwala każdemu, kto może złożyć jakikolwiek wniosek o certyfikat, wpisać w SAN dowolną nazwę, także konta uprzywilejowanego (ESC6), a „na chwilę” często zostaje na lata,

jak opisuje strona Hartowanie AD CS: ESC1 do ESC16 po ludzku, uprawnienia, audyt i kopia klucza. Flaga nie jest zresztą potrzebna: wystawiamy certyfikat z szablonu `ZielonaWWW`, w którym nazwę podaje się w żądaniu, a SAN wpisujemy w żądanie jako rozszerzenie w `request.inf` albo `san.cnf`. Wniosek zatwierdza menedżer certyfikatów, a przed importem na `fw01` sprawdzamy SAN poleceniem `certutil -dump`.

Źródła: Always On VPN Error 13801, Richard M. Hicks Consulting · Always On VPN Error 13806, Richard M. Hicks Consulting · Common VPN Error Codes and How to Fix Them, Astrill VPN · Always On VPN User Tunnel Error 812, Microsoft Q&A · Import a certificate, Fortinet Document Library · ESC6, Request Attribute SAN (EDITF_ATTRIBUTESUBJECTALTNAME2), SpecterOps

---

Revision #27
Created 2026-09-28 06:15:11 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:10 UTC by Tomasz Konieczny