EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD

Poziom: zaawansowany

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

Czas: ~40 min

Docelowy sposób logowania do VPN w Zielonej to certyfikat użytkownika zamiast hasła, a dostęp do zasobów w LAN sterowany tymi samymi grupami Active Directory, których używa się przy zwykłym logowaniu w biurze. Ta strona pokazuje, jak dojść do tego stanu i jak go potem utrzymać.

ZAŁOŻENIA SCENARIUSZA

tunel kończy się na pojedynczym `fw01` z jednym łączem (`wan1`, 203.0.113.10). Kolektor FSSO na `dc01` i serwer NPS na `dc02` stoją w VLAN 10 i są osiągalne z `fw01` w tej samej serwerowni, bez tunelu między lokalizacjami.

Skróty użyte na tej stronie (13)

Skrót	Co znaczy
AD CS	Active Directory Certificate Services: rola Windows Server pełniąca funkcję firmowego urzędu certyfikacji
DC	Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników
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
LAN	Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe

Skrót	Co znaczy
NPS	Network Policy Server: rola Windows Server obsługująca RADIUS, pośredniczy w sprawdzaniu hasła domenowego przy logowaniu do VPN albo Wi-Fi
SAN	w certyfikatach: Subject Alternative Name, dodatkowe nazwy hosta w certyfikacie; w pamięciach: Storage Area Network, sieć dyskowa
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
UPN	User Principal Name: login w formie adresu, np. jan.nowak@zielona.example
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

□□ ZMIENIA SYSTEM

Rejestracja kolektora FSSO na bramie: config user fsso

```
config user fsso
    edit "FSSO_Zielona"
        set server "dc01.ad.zielona.example"
        set port 8000
        set password HasloKolektoraFsso
    next
end
```

Rejestruje na `fw01` adres i hasło kolektora FSSO działającego na `dc01`, na domyślnym porcie `8000`. Od tego momentu brama zaczyna otrzymywać od kolektora informację, kto i z jakiej grupy właśnie się zalogował w sieci Zielonej.

□□ **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 · **config** = FortiOS: otwiera blok ustawień jednej tabeli konfiguracji, na przykład config system ha, i kończy się słowem end

□□ TYLKO ODCZYT

Sprawdzenie połączenia z kolektorem FSSO: diagnose debug authd fsso server-status

```
diagnose debug authd fsso server-status
```

Pokazuje, czy `fw01` widzi kolektor FSSO jako połączony, i od kiedy. Pierwsze polecenie po każdej zmianie hasła albo adresu kolektora, zanim zaczniemy szukać przyczyny gdzie indziej.

Przykład:

```
Server Name: FSSO_Zielona
Connection status: connected
Connected since: Mon Sep 28 08:12:03 2026
```

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 · **diagnose** = FortiOS: polecenia diagnostyczne zapory i zarządzanych przełączników, na przykład diagnose sys sdwan member pokazuje członków SD-WAN

ZMIENIA SYSTEM

Grupa dopuszczająca do zasobów LAN według FSSO: config user group

```
config user group
    edit "FSSO_Handlowcy"
        set group-type fsso-service
        set member "ZIELONA/Handlowcy"
    next
end
```

Tworzy na `fw01` grupę firewallową odzwierciedlającą grupę domenową `Handlowcy`, rozpoznawaną wyłącznie po tym, że FSSO widziała logowanie danej osoby, bez pytania jej o dodatkowe hasło do samej zapory.

LAN = Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe · **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 · **config** = FortiOS: otwiera blok ustawień jednej tabeli konfiguracji, na przykład config system ha, i kończy się słowem end

⚠ ZMIENIA SYSTEM

Uwierzytelnienie EAP-TLS w tunelu IKEv2: config vpn ipsec phase1-interface

```
config vpn ipsec phase1-interface
    edit "vpn_zielona_user"
        set type dynamic
        set interface "wan1"
        set ike-version 2
        set peertype peer
        set mode-cfg enable
        set proposal aes256-sha256
        set dhgrp 14
        set eap enable
        set eap-identity send-request
        set authusrgrp "VPN_Zielona_Uzytkownicy"
        set certificate "vpn.zielona.example"
    next
end
```

Włącza uwierzytelnianie EAP w tunelu dopuszczającym, jednocześnie sprawdzając certyfikat po stronie klienta (`peertype peer`) i ograniczając dopuszczonych do grupy `VPN_Zielona_Uzytkownicy`, powiązanej w Active Directory z `GG_VPN_Uzytkownicy`. `authusrgrp` ustawiamy tutaj albo w polityce firewall, nigdy w obu miejscach naraz.

EAP-TLS = EAP z TLS: uwierzytelnianie certyfikatem użytkownika albo urządzenia zamiast hasła · **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 · **EAP** = Extensible Authentication Protocol: rodzina metod uwierzytelniania, dzięki której VPN albo Wi-Fi mogą pytać o hasło albo o certyfikat na wiele różnych sposobów · **config** = FortiOS: otwiera blok ustawień jednej tabeli konfiguracji, na przykład config system ha, i kończy się słowem end

⚠ ZMIENIA SYSTEM

Polityka firewall łącząca VPN z LAN według grup FSSO: config firewall policy

```
config firewall policy
    edit 0
```

```
        set name "VPN-Zielona-do-LAN"
        set srcintf "vpn_zielona_user"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set groups "FSSO_Handlowcy"
        set nat enable
    next
end
```

Wpuszcza ruch z tunelu do sieci wewnętrznej wyłącznie dla osób, których FSSO oznaczyła jako członków grupy `Handlowcy`. Sam fakt otwarcia tunelu (grupa `VPN_Zielona_Uzytkownicy` z fiszki wyżej) i dostęp do konkretnych zasobów w LAN (grupa `FSSO_Handlowcy` tutaj) to dwie oddzielne, niezależne bramki.

VPN = Virtual Private Network: szyfrowany tunel do sieci firmowej · **LAN** = Local Area Network: sieć lokalna; w BMC port LAN to jego własne gniazdo sieciowe · **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 · **config** = FortiOS: otwiera blok ustawień jednej tabeli konfiguracji, na przykład config system ha, i kończy się słowem end

Z życia wzięte

Z ŻYCIA WZIĘTE

Ola zgłasza, że jej zespół programistów po połączeniu VPN nie widzi udziału z repozytoriami na `docker01`, choć sama VPN się łączy bez problemu. Tomek sprawdza `diagnose debug authd fsso server-status` i widzi kolektor jako połączony, ale w polityce firewall `VPN-Zielona-do-LAN` wciąż stoi stara grupa `FSSO_Handlowcy`, bez nowo utworzonej grupy domenowej `Programisci`, do której Ola i jej zespół zostali niedawno przeniesieni.

Jak to działa

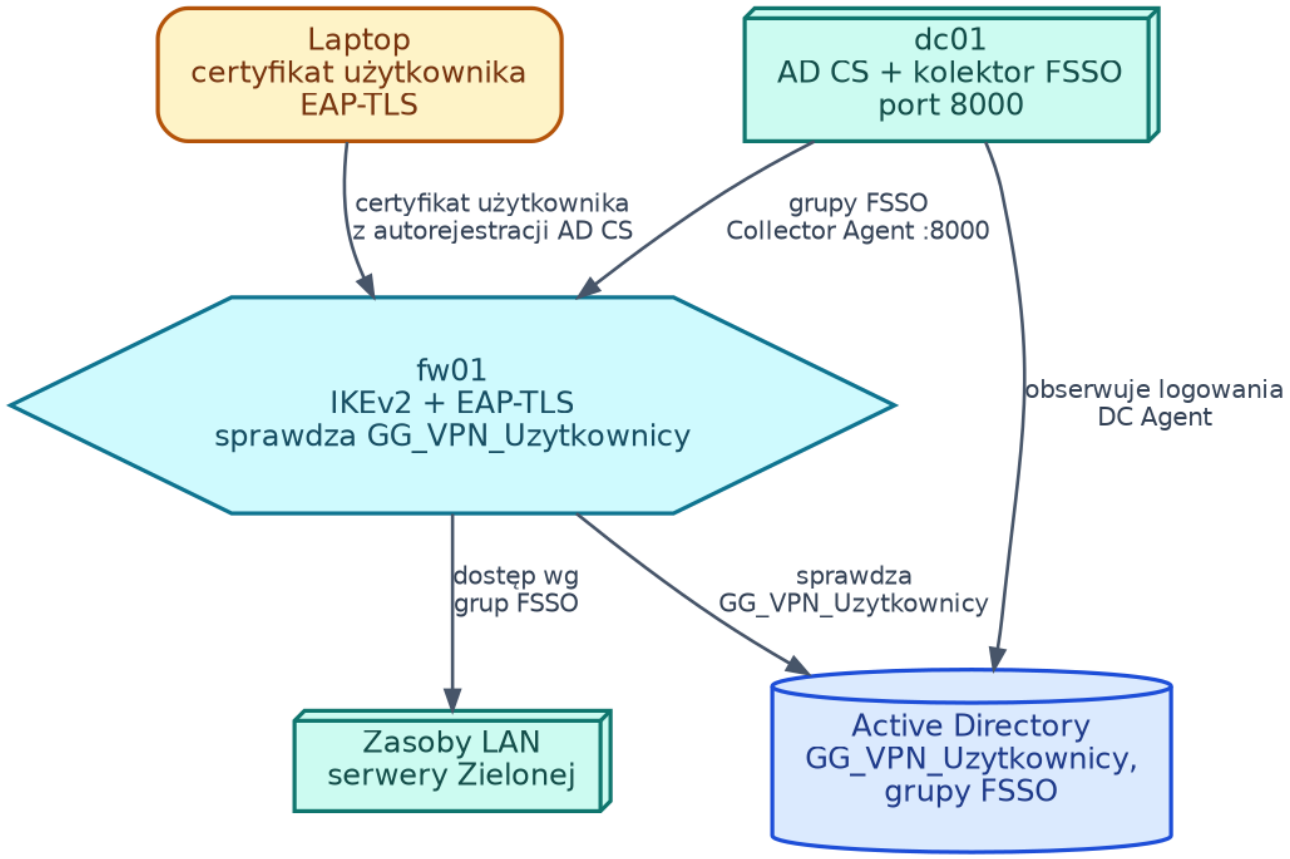
▯▯ Rozwiń: jak to działa pod spodem

Droga do dzisiejszego stanu w Zielonej prowadziła przez trzy kolejne metody logowania do VPN, każda usuwała jedną niedogodność poprzedniej. Najpierw stał klasyczny **EAP-PEAP z MSCHAPv2**: użytkownik podawał swoje zwykłe hasło domenowe, `fw01` przekazywał je do serwera **NPS** (rola Windows Server obsługująca **RADIUS**) na `dc02`, a ten sprawdzał je w Active Directory. Działało, ale każde wygaśnięcie albo zmiana hasła domenowego oznaczała telefon od kogoś, kto nie mógł się połączyć z hotelu.

Drugim krokiem było uwierzytelnianie podpisem, z wyłączonym EAP: `fw01` sam sprawdzał certyfikat klienta, a peer wyszukiwał pasujące konto po UPN zapisanym w polu SAN certyfikatu. To usuwało problem haseł, ale wymagało ręcznego wystawiania certyfikatów każdej nowej osobie, więc nie skalowało się dobrze na kilkudziesięciu handlowców.

Kierunkiem docelowym, opisanym w tej fiszce, jest **EAP-TLS** z certyfikatami użytkowników wystawianymi automatycznie: szablon certyfikatu w AD CS z włączoną autorejestracją zapisuje certyfikat na koncie użytkownika bez udziału administratora, przy najbliższym odświeżeniu zasad grupy. Obok tego działa klasyczne **FSSO** (DC Agent obserwujący logowania na kontrolerach domeny plus Collector Agent na `dc01:8000`), dzięki któremu autoryzacja dostępu do zasobów LAN działa dokładnie tymi samymi grupami co w biurze, bez osobnego zestawu reguł dla samego VPN.

Szablon certyfikatu użytkownika (`ZielonaUzytkownik`, z UPN w SAN i rozszerzeniem SID) i automatyczną rejestrację opisuje strona Szablony, automatyczna rejestracja i silne mapowanie certyfikatów. Laptopy, które nie widzą kontrolera domeny, dostają certyfikat przez Intune według strony Certyfikaty, Wi-Fi i VPN z Intune: Certificate Connector czy Cloud PKI. Druga strona tunelu, czyli certyfikat, którym przedstawia się sama brama `fw01`, ma własne wymagania co do EKU i SAN, zebrane na stronie Błąd 13801: certyfikat bramy VPN, EKU i SAN.



Schemat autoryzacji: certyfikat użytkownika otwiera tunel, FSSO z dc01 daje dostęp do zasobów LAN według grup (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: FSSO.** Fortinet Single Sign-On, mechanizm łączący FortiGate z Active Directory tak, że brama wie, kto jest zalogowany i do jakich grup należy, obserwując logowania w domenie zamiast pytać samą osobę o dodatkowe hasło do zapory.

Rozdział ról jest tu celowy i dwustopniowy. Grupa `GG_VPN_Uzytkownicy` w Active Directory, odzwierciedlona na `fw01` jako `VPN_Zielona_Uzytkownicy`, odpowiada wyłącznie za pierwszą bramkę: czy dane konto w ogóle może otworzyć tunel do internetu i kontrolerów domeny. Grupy FSSO, takie jak `Handlowcy` czy `Programisci`, odpowiadają za drugą, niezależną bramkę: do jakich konkretnie zasobów w sieci lokalnej to konto ma dostęp, już po otwarciu tunelu. Dodanie kogoś do jednej grupy nigdy nie zastępuje dodania go do drugiej.

Częste błędy

Objaw	Przyczyna	Co robimy
`diagnose debug authd fsso server-status` pokazuje kolektor jako rozłączony	zła nazwa hosta, port inny niż `8000` albo nieaktualne hasło kolektora w `config user fsso`	poprawiamy dane w `config user fsso`, sprawdzamy zaporę między `fw01` a `dc01` na porcie `8000`
Osoba należy do właściwej grupy domenowej, ale polityka firewall jej nie wpuszcza	grupa FSSO na `fw01` nie została odświeżona po zmianie członkostwa w Active Directory	wymuszamy odświeżenie komendą `diagnose debug authd fsso refresh-groups` albo `execute fsso refresh`
Tunel łączy się certyfikatem, ale zaraz potem żąda dodatkowo hasła EAP	w `phase1-interface` włączone jednocześnie `eap enable` i osobne uwierzytelnienie hasłem w tej samej negocjacji zamiast jednego spójnego mechanizmu	ustalamy jedną metodę uwierzytelnienia użytkownika na tunel, zgodnie z tabelą metod ze strony o pojęciach IPsec i IKEv2
Nowa osoba w zespole nie dostaje certyfikatu do EAP-TLS mimo dodania do grupy autorejestracji	zasady grupy z autorejestracją certyfikatów jeszcze się nie odświeżyły na jej koncie	wymuszamy `gpupdate /force` na stacji i sprawdzamy w `certmgr.msc`, czy certyfikat pojawił się w magazynie użytkownika

□□ Ćwiczenia

1. Marek z magazynu w Swarzędzu należy do grupy `GG_VPN_Uzytkownicy`, więc VPN łączy mu się bez problemu, ale po połączeniu nie widzi udziału plikowego na `fs01`. Gdzie szukamy przyczyny w pierwszej kolejności?

Odpowiedź

Sprawdzamy grupy FSSO, nie samą konfigurację tunelu. Grupa `GG_VPN_Uzytkownicy` odpowiada wyłącznie za otwarcie tunelu, a dostęp do konkretnych zasobów LAN, takich jak udział na `fs01`, zależy od osobnej grupy FSSO w polityce firewall. Marek mógł nie zostać jeszcze dodany do właściwej grupy domenowej albo `fw01` nie odświeżyło jeszcze jego członkostwa.

1. Dlaczego przejście z uwierzytelnienia hasłem (EAP-PEAP/MSCHAPv2) na uwierzytelnienie certyfikatem użytkownika (EAP-TLS) zmniejsza liczbę zgłoszeń o niedziałającym VPN?

Odpowiedź

Bo znika najczęstsza przyczyna takich zgłoszeń: wygasłe albo niedawno zmienione hasło domenowe. Certyfikat użytkownika z autorejestracji AD CS odnawia się automatycznie w tle, bez udziału samego użytkownika, więc przestaje być czynnikiem, który może akurat wygasnąć w dniu wyjazdu w teren.

Źródła: config user fsso, Fortinet Document Library · IPsec IKEv2 VPN 2FA with EAP and certificate authentication, Fortinet Document Library · Technical Tip: Useful FSSO Commands, Fortinet Community · Technical Tip: Configure FSSO in DC Agent mode, Fortinet Community

---

Revision #27
Created 2026-09-28 06:15:14 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:13 UTC by Tomasz Konieczny