**cw15: Izolacja konta domenowego FTP/FTPS (AD + GPO + NTFS + IIS)**

Data opracowania: 2026-02-07

**Cel ogólny lekcji** Uczeń wykonuje konfigurację i zabezpieczenie dostępu do usługi **FTP/FTPS** w środowisku domenowym poprzez zastosowanie **grupy AD**, **GPO (blokady logowania)**, **uprawnień NTFS** oraz **reguł autoryzacji w IIS**, a następnie weryfikuje działanie konfiguracji testami (w tym błędami 530/550).

**Cele szczegółowe lekcji** Po lekcji uczeń potrafi:

✓ Utworzyć grupę zabezpieczeń **GG_FTP_Users** i dodać do niej użytkownika domenowego **ftpadmin**.

✓ Utworzyć i podpiąć obiekt **GPO_FTP_Isolation** do domeny oraz zastosować **filtrowanie zabezpieczeń** tak, aby polityka dotyczyła wskazanego serwera (konto komputera) i miała uprawnienia **Odczyt** oraz **Stosowanie zasad grup**.

✓ Skonfigurować w GPO prawa użytkownika (Przypisywanie praw użytkownika):

- **Odmowa logowania lokalnego**,
- **Odmowa logowania za pomocą usług pulpitu zdalnego**,
- **Uzyskiwanie dostępu do tego komputera z sieci** dla grupy **GG_FTP_Users**.

✓ Utworzyć katalog domowy FTP użytkownika i nadać uprawnienia NTFS (z użyciem icacls) zapewniające izolację danych dla **GG_FTP_Users** oraz administratorów.

✓ Zweryfikować/ustawić w IIS wymagane elementy dostępu do FTP/FTPS (uwierzytelnianie podstawowe włączone, anonimowe wyłączone; autoryzacja dla grupy domenowej).

✓ Wykonać i udokumentować testy weryfikacyjne konfiguracji: brak logowania lokalnego i RDP dla ftpadmin, poprawne połączenie FTPS, brak dostępu do obcych katalogów (550) oraz odmowa połączenia dla użytkownika spoza grupy (530).

## 2. Stan początkowy (wymagany)

Wykonaj poniższe polecenia celem przygotowania środowiska:

Jednorazowo przywróć punkty kontrolne z kontrolerem domeny z 11 podłaczona do domeny.

Na kontrolerze domeny  Uruchom jako Administrator PowerShell ISE i uruchamiaj kolejno:

a. Instalacja IIS + FTP

*Install-WindowsFeature Web-Server, Web-Ftp-Server -IncludeManagementTools*

b. Lokalny użytkownik ftpadmin

```
$pass = ConvertTo-SecureString "zaq1@WSX" -AsPlainText -Force
if (-not (Get-LocalUser -Name ftpadmin -ErrorAction SilentlyContinue)) {
    New-LocalUser ftpadmin -Password $pass -PasswordNeverExpires:$true
}
```

c. Katalog ftproot + NTFS

```
$root = "C:\inetpub\ftproot"
New-Item -ItemType Directory -Force -Path $root
icacls $root /grant "ftpadmin:(OI)(CI)F"
```

d. Certyfikat TLS

```
$cert = New-SelfSignedCertificate `
  -DnsName "ftp.local" `
  -CertStoreLocation Cert:\LocalMachine\My
```

e. Witryna FTP

```
Import-Module WebAdministration
if (-not (Test-Path IIS:\Sites\FTPS)) {
    New-WebFtpSite -Name "FTPS" -Port 21 -PhysicalPath $root
}
```

f. Wymuszenie TLS – FTPS Explicit

```
Set-ItemProperty `
  IIS:\Sites\FTPS `
  -Name ftpServer.security.ssl.controlChannelPolicy `
```

*-Value Require*

*Set-ItemProperty `*

*IIS:\Sites\FTPS `*

*-Name ftpServer.security.ssl.dataChannelPolicy `*

*-Value Require*

*Set-ItemProperty `*

*IIS:\Sites\FTPS `*

*-Name ftpServer.security.ssl.serverCertHash `*

*-Value $cert.Thumbprint*

g. Uwierzytelnienie i autoryzacja (cw13–14)

*& "$env:windir\System32\inetsrv\appcmd.exe" unlock config `*

*-section:system.ftpServer/security/authentication/basicAuthentication*

*& "$env:windir\System32\inetsrv\appcmd.exe" unlock config `*

*-section:system.ftpServer/security/authorization*

*Add-WebConfiguration `*

*"/system.ftpServer/security/authentication/basicAuthentication" `*

*-Value @{enabled="true"} -PSPath IIS:\Sites\FTPS*

*Add-WebConfiguration `*

*"/system.ftpServer/security/authorization" `*

*-Value @{accessType="Allow";roles="";users="ftpadmin";permissions="Read,Write"} `*

*-PSPath IIS:\Sites\FTPS*

h. Zapora – tylko port 21

*New-NetFirewallRule -DisplayName "FTPS-Control" `*

*-Direction Inbound -Protocol TCP -LocalPort 21 -Action Allow*

Efekt przygotowania:
Ćwiczenie wykonujesz na serwerze, na którym środowisko zostało przygotowane (FTPS działa).
Serwer jest w domenie (w tym scenariuszu: kontroler domeny).
W IIS istnieje witryna FTP/FTPS (np. „FTPS") i działa połączenie FTPS (Explicit TLS).
W IIS: Uwierzytelnianie podstawowe – Włączone; Uwierzytelnianie anonimowe – Wyłączone.
W domenie istnieje konto użytkownika: ftpadmin (domenowe).

**3. Materiały i narzędzia**

Serwer: Menedżer usług IIS, Zarządzanie zasadami grupy (GPMC), Active Directory Users and Computers.
Klient: FileZilla i/lub WinSCP (FTPS Explicit TLS).
CMD/PowerShell (Administrator) do gpupdate i icacls.

**4.1. Treść zadania**

Celem zadania jest skonfigurowanie bezpiecznego środowiska FTPS opartego o Active Directory oraz wykazanie działania izolacji użytkowników i kontroli dostępu.
Masz działający serwer **FTPS**. Twoim zadaniem jest:

1. **Zintegrować usługę FTP z Active Directory**
2. **Skonfigurować izolację użytkowników** (AD + IIS + NTFS)
3. **Udowodnić poprawność i bezpieczeństwo konfiguracji** poprzez wykonanie testów (530, 550, FTPS, brak logowania lokalnego/RDP)

**4.2 Wykonaj zadanie w kolejnych etapach**

**Etap 1. Utworzenie grupy zabezpieczeń i przypisanie użytkownika**

1. Otwórz „Active Directory Users and Computers".
2. W kontenerze „Users" (lub wskazanej lokalizacji) utwórz grupę: GG_FTP_Users (Typ: Zabezpieczenia, Zakres: Globalna).
3. Dodaj użytkownika domenowego ftpadmin do grupy GG_FTP_Users.
   Add-ADGroupMember GG_FTP_Users ftpadmin

**Uwaga:** Od tego momentu uprawnienia nadajemy grupie, a nie bezpośrednio użytkownikowi.

**Etap 2. Utworzenie GPO ograniczającego logowanie kont FTP (działa tylko na serwerze FTP)**

1. Otwórz „Zarządzanie zasadami grupy” (**gpmc.msc**).
2. Utwórz nowy obiekt GPO o nazwie: GPO_FTP_Isolation.
3. Podłącz (Link) GPO GPO_FTP_Isolation do domeny rol00.edu.pl.
4. W „Filtrowanie zabezpieczeń” usuń „Użytkownicy uwierzytelnieni”.
5. Dodaj konto komputera serwera FTP (np. ROL$).
6. Upewnij się (na zakładce Delegowanie), że konto komputera ma uprawnienia: Odczyt oraz Stosowanie zasad grup.

**Etap 3. Blokady logowania (Przypisywanie praw użytkownika)**

Otwórz **Zarządzanie zasadami grupy** (gpmc.msc).

Wybierz utworzone wcześniej GPO (np. GPO_FTP_Isolation) i kliknij **Edytuj**.

Przejdź ścieżką:

Konfiguracja komputera

└ Zasady

└ Ustawienia systemu Windows

└ Ustawienia zabezpieczeń

└ Zasady lokalne

└ Przypisywanie praw użytkownika

Skonfiguruj:

a. Odmowa logowania lokalnego > dodaj: IS\GG_FTP_Users

b. Odmowiaj logowania za pomocą usług pulpitu zdalnego > dodaj: IS\GG_FTP_Users

c. Uzyskiwanie dostępu do tego komputera z sieci > dodaj: IS\GG_FTP_Users

**Uwaga:** Po zmianach wymuś aktualizację zasad na serwerze: gpupdate /force

**Etap 4. Izolacja danych – NTFS**

Utwórz katalog domowy FTP dla ftpadmin zgodnie z konwencją domenową:

C:\inetpub\ftproot\<NETBIOS_DOMENY>\ftpadmin

C:\inetpub\ftproot\ROL\ftpadmin

Nadaj uprawnienia NTFS (przykład dla domeny rol):

icacls "C:\inetpub\ftproot\ROL\ftpadmin" /inheritance:r

icacls "C:\inetpub\ftproot\ROL\ftpadmin" /grant "rol00\GG_FTP_Users:(OI)(CI)M"

icacls "C:\inetpub\ftproot\ROL\ftpadmin" /grant "Administratorzy:(OI)(CI)F"

**Uwaga:** Jeśli NETBIOS domeny jest inny, zamień „ROL” na właściwą nazwę.

**Efekt:**

- ftpadmin widzi tylko swój katalog (bo IIS izoluje użytkowników wg %UserDomain%\%UserName%)
- nie ma dostępu do system (bo GPO blokuje logowanie lokalne i RDP)
- dostęp wyłącznie sieciowy (FTP/FTPS)

**Etap 5. IIS – autoryzacja FTP dla grupy**

1. Otwórz Menedżera usług IIS > Witryny > wybierz witrynę FTP (np. FTPS).
2. Otwórz „Uwierzytelnianie FTP”: upewnij się, że Uwierzytelnianie podstawowe jest **Włączone**, a Anonimowe – **Wyłączone**.

**Efekt końcowy**

- IIS korzysta z Active Directory, bo:
  – Basic Authentication na kontrolerze domeny uwierzytelnia użytkowników AD
- Logowanie lokalnymi kontami nie działa, bo:
  – w domenie konta lokalne są ignorowane, gdy dostęp odbywa się przez usługę opartą o AD

IIS używa Active Directory (nie kont lokalnych).

3. Otwórz „Reguły autoryzacji FTP”: usuń reguły, które nie są potrzebne (np. All Users/Anonymous).
4. Dodaj regułę „Zezwalaj”: Określone role lub grupy użytkowników > wpisz: IS\GG_FTP_Users.
5. Zaznacz uprawnienia: Odczyt oraz Zapis.

**Etap 6. Testy obowiązkowe (weryfikacja izolacji)**

Przygotowanie (żeby testy były miarodajne)

1. Zastosuj GPO na serwerze (DC/FTP):

Otwórz Wiersz polecenia jako Administrator i uruchom: gpupdate /force

2. Sprawdź, że użytkownik jest w grupie GG_FTP_Users:

Na serwerze (PowerShell):

Get-ADUser ftpadmin -Properties MemberOf | Select-Object -ExpandProperty MemberOf

albo w GUI: Active Directory Users and Computers > Users > ftpadmin > Członek grupy.

3. Miej pod ręką dane do testu FTPS (np. FileZilla/WinSCP na kliencie):

- Serwer/Host: IP (np. 192.167.0.1) lub nazwa (np. ftp.rol.edu.pl)
- Port: 21
- Protokół: **FTP**
- Szyfrowanie: **Wymuś explicit TLS/SSL (FTPS)**
- Login/hasło: ftpadmin / Twoje hasło.

Wykonaj i udokumentuj poniższe testy:

**TEST 1:**

Logowanie lokalne jako ftpadmin > oczekiwane: błąd/odmowa uruchomienia (w zależności od polityk).

W CMD: runas /user:rol00\ftpadmin cmd Podaj hasło.

**TEST 2:**

Logowanie przez RDP jako ftpadmin > oczekiwane: odmowa

Na kliencie (Windows 10/11) uruchom:

Połączenie pulpitu zdalnego (**mstsc**)

Wpisz adres serwera (IP/nazwa).

Login: rol00\ftpadmin

Hasło: (Twoje)

Kliknij Połącz.

**TEST 3:**

Połączenie FTPS (FileZilla/WinSCP, Explicit TLS) jako ftpadmin > oczekiwane: sukces

***FileZilla (zalecane)***

Otwórz FileZilla > Menedżer stron

Utwórz wpis:

Host: IP/nazwa serwera

Port: **21**

Protokół: **FTP**

Szyfrowanie: **Wymagaj jawnego FTP przez TLS (Explicit)**

Typ logowania: Normalny

Użytkownik: **ftpadmin** (lub rol00\ftpadmin, zależnie jak logujesz)

Hasło: …

Połącz.

***WinSCP (alternatywa)***

Protokół: **FTP**

Szyfrowanie: **Jawne TLS/SSL**

Login: **ftpadmin**

**TEST 4:**

Próba dostępu do innego katalogu (poza własnym) > oczekiwane: błąd 550 / brak dostępu

Tu sprawdzasz, czy izolacja + NTFS działa.

W FileZilla

Połącz się jako **ftpadmin**.

Spróbuj wejść „wyżej" (do katalogu nadrzędnego):

kliknij **..** jeśli widać

albo wpisz w „Zdalna ścieżka" coś typu:

/

**/ROL**

**/ftpuser2**

Spróbuj też:

utworzyć katalog poza swoim katalogiem (jeśli widzisz coś więcej)

Jeśli przypadkiem widzi inne katalogi:

- sprawdź w IIS: Izolacja użytkowników FTP (powinna być opcja izolująca)
- sprawdź ACL NTFS: czy nie dałeś zbyt szerokich praw grupie na katalog nadrzędny.

**TEST 5:**

Próba połączenia innym użytkownikiem AD spoza IS\GG_FTP_Users > oczekiwane: odmowa (530)

Ten test ma pokazać, że nie każdy user AD ma wejście, nawet jeśli istnieje w domenie.

Przygotuj użytkownika testowego (np. **adtest1**) – który NIE jest w GG_FTP_Users

```
Import-Module ActiveDirectory
$pass = ConvertTo-SecureString "zaq1@WSX" -AsPlainText -Force
$dn = (Get-ADDomain).DistinguishedName
if (-not (Get-ADUser -Filter "SamAccountName -eq 'adtest1'" -ErrorAction SilentlyContinue)) {
  New-ADUser `
    -Name "AD Test 1" `
    -SamAccountName "adtest1" `
```

```
    -UserPrincipalName "adtest1@$((Get-ADDomain).DNSRoot)" `
    -AccountPassword $pass `
    -Enabled $true `
    -PasswordNeverExpires $true `
    -ChangePasswordAtLogon $false `
    -Path "CN=Users,$dn" `
    -Description "Konto testowe do negatywnego testu FTP/FTPS – poza GG_FTP_Users"
  Write-Host "Utworzono adtest1" -ForegroundColor Green
}
else {
  Write-Host "adtest1 już istnieje – pomijam tworzenie" -ForegroundColor Yellow
}
```

Upewnij się, że: konto istnieje w AD, NIE należy do GG_FTP_Users, nie ma indywidualnej reguły „Allow” w IIS

Test (FileZilla / WinSCP)

1. Zmień login na rol00\adtest1
2. Spróbuj połączyć się FTPS.

**7. Dowody do oddania**

Screen odmowy logowania lokalnego (komunikat).

Screen odmowy logowania RDP (komunikat).

Screen udanego połączenia FTPS (widoczne TLS + listing katalogu).

Screen błędu dostępu (np. 550) przy próbie wejścia do innego katalogu.

Screen odmowy logowania użytkownika AD spoza grupy (530 w kliencie).

Krótka notatka (5–7 zdań): dlaczego zastosowano grupę, GPO i NTFS oraz jakie to daje bezpieczeństwo.

**8. Pytania kontrolne (wnioski)**

1. Dlaczego poprawne hasło nie wystarcza do logowania (podaj 2 powody)?
2. Jaka jest różnica między izolacją w IIS a izolacją przez NTFS?
3. Dlaczego konta FTP nie powinny mieć prawa logowania lokalnego/RDP?
4. Co oznacza błąd 530, a co 550 w kontekście FTP/FTPS?