GOPAS | DAQUAS | Microsoft

Generální partner
ATOM

Fiddler

Ing. Ondřej Ševeček | GOPAS a.s.
MCSM:Directory | MVP:Security | CISA | CISM | CEH | CHFI | CISSP
ondrej@sevecek.com | www.sevecek.com

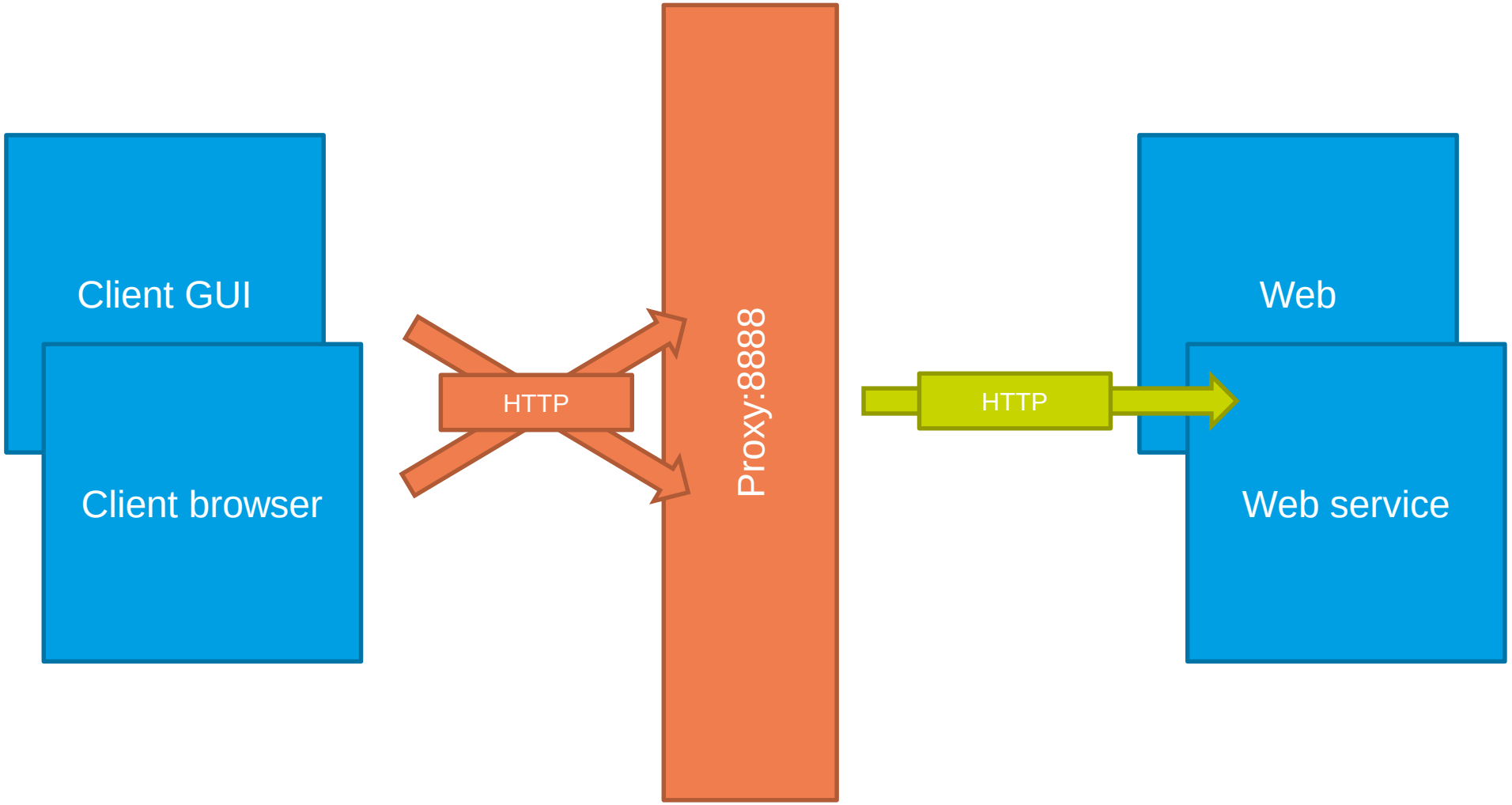
relevantní kurzy:
GOC166 (ADFS), GOC168 (IIS), GOC169 (ISO 2700x)

14. - 17. května 2018
Tech·Ed DevCon
PRAHA 2018

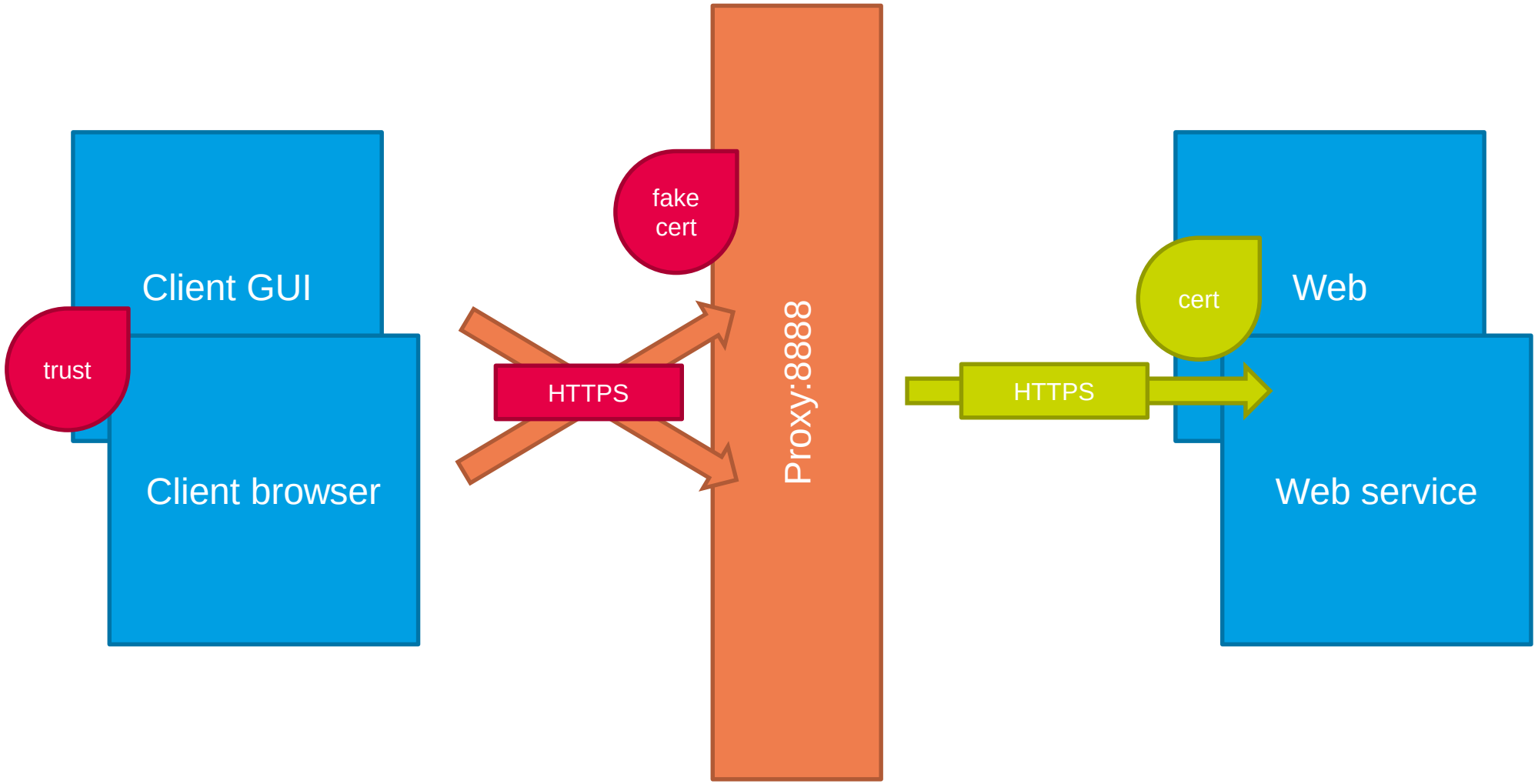
Motivation

- Browsers
  - IE, Edge, Chrome, ...
- Non-browser clients
  - winhttp, Java, ...
  - Outlook, Word, Excel, web service clients, ...
- User accounts
  - my own user, SYSTEM, Network Service, Local Service, ...

HTTP web proxy



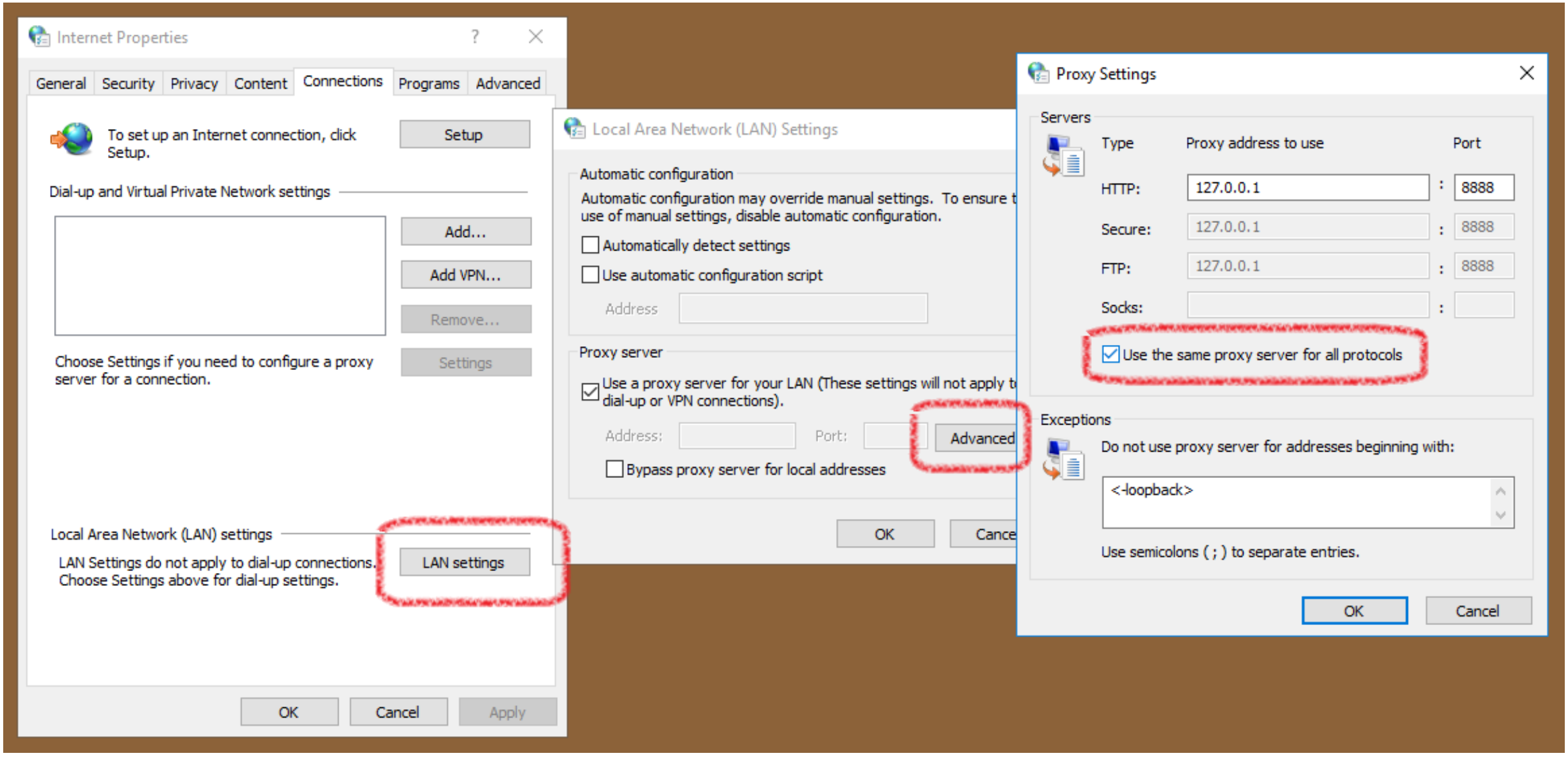
SSL proxy


Client GUI
trust
Client browser
fake
cert
HTTPS
Proxy:8888
cert
Web
HTTPS
Web service

Local debugging

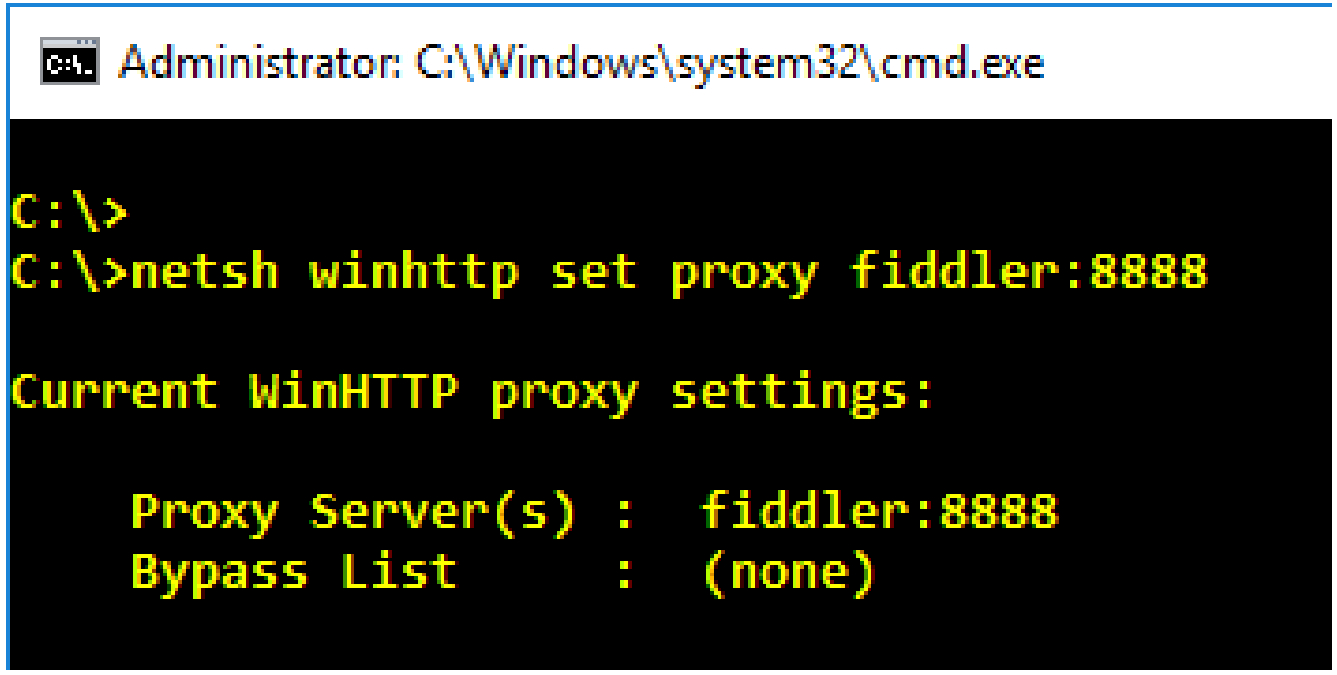
Fiddler

Change proxy settings to all protocols

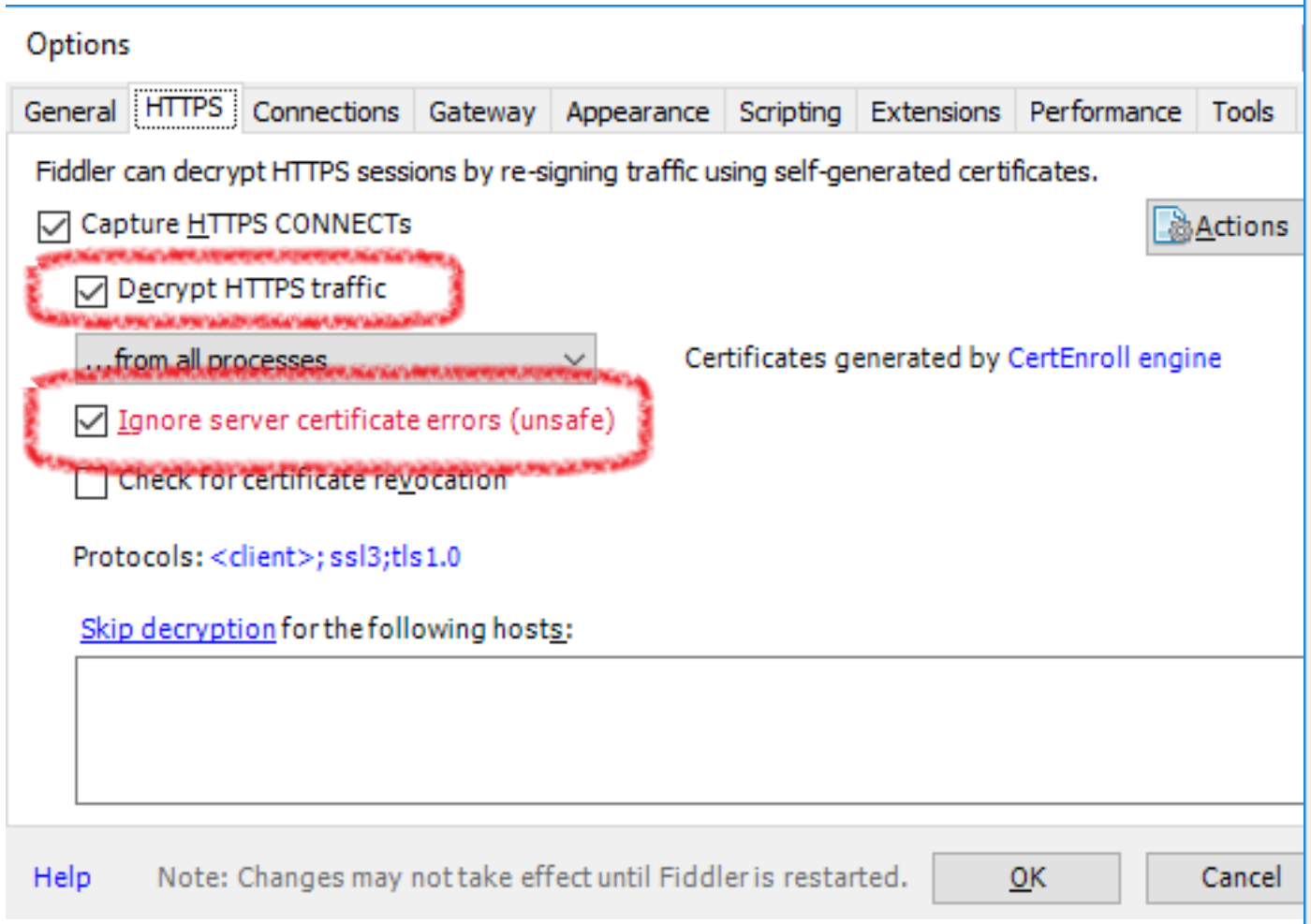


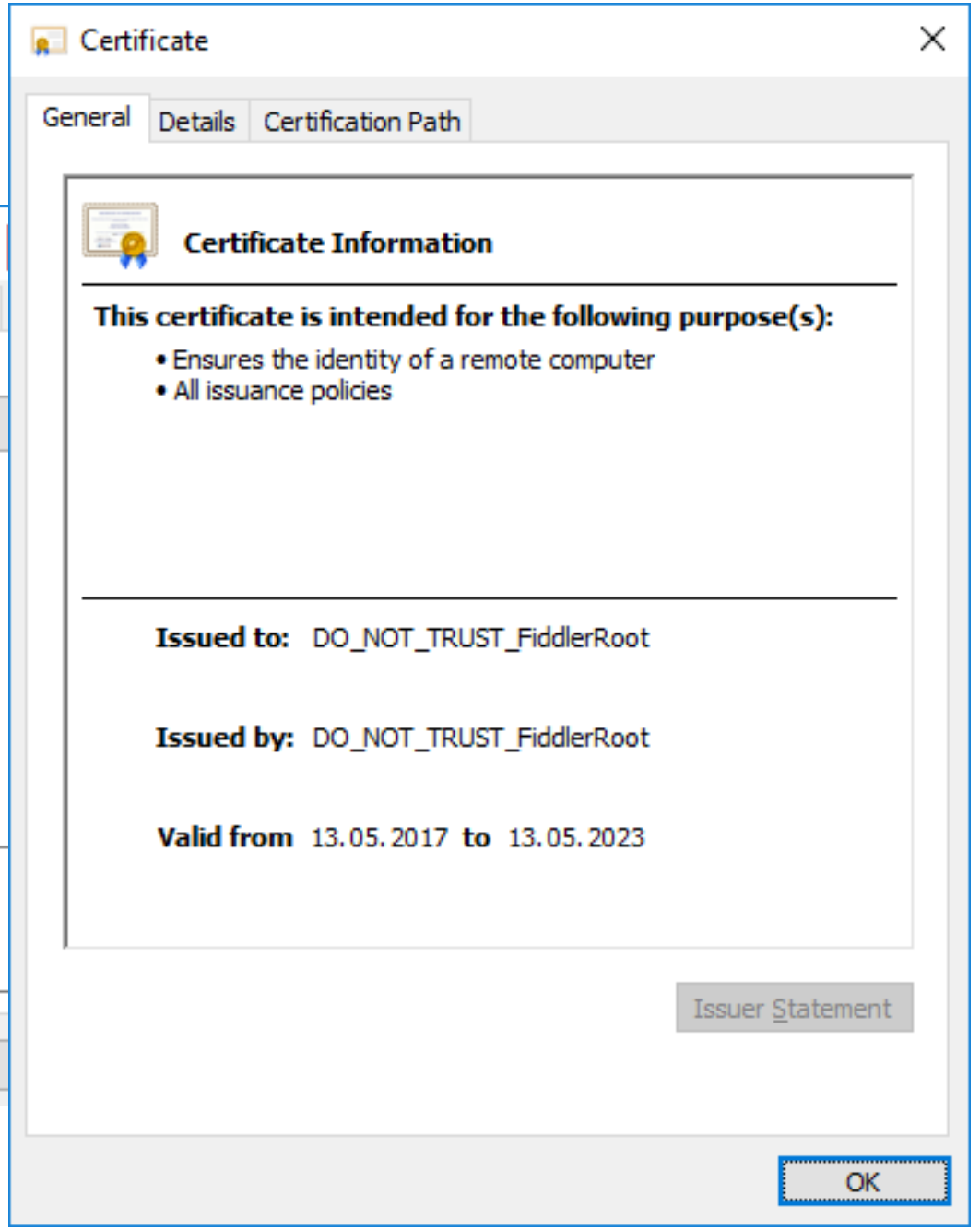
Configure old winhttp SYSTEM clients

- netsh winhttp set proxy



Enable SSL inspection



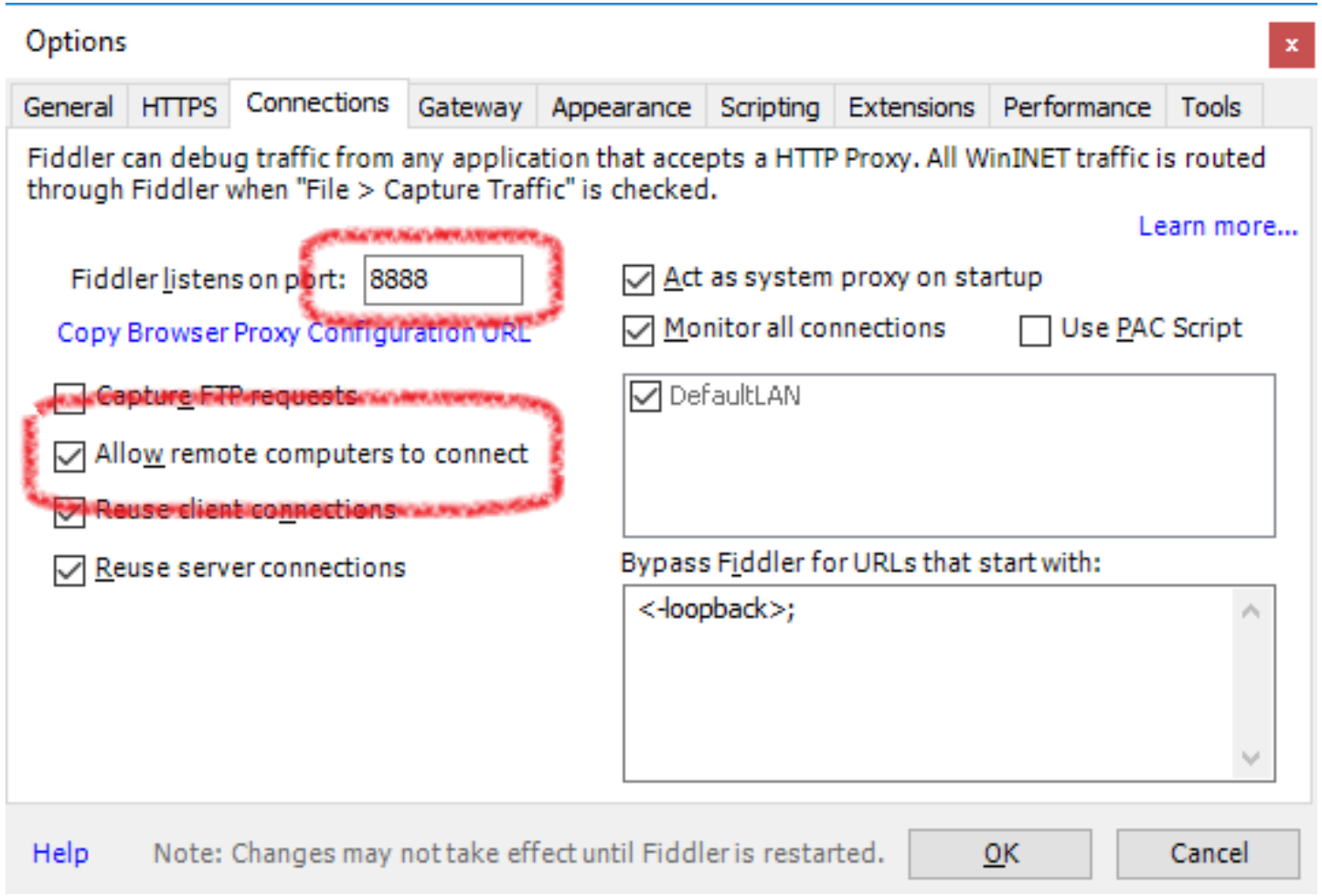


GOPAS | DAQUAS | Microsoft

Remote debugging is smoother

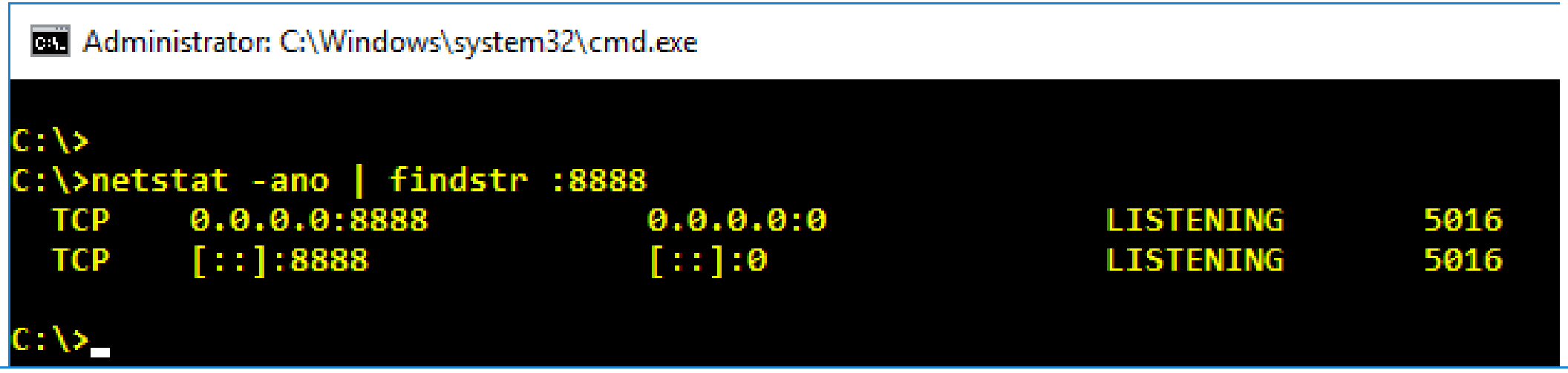
Fiddler

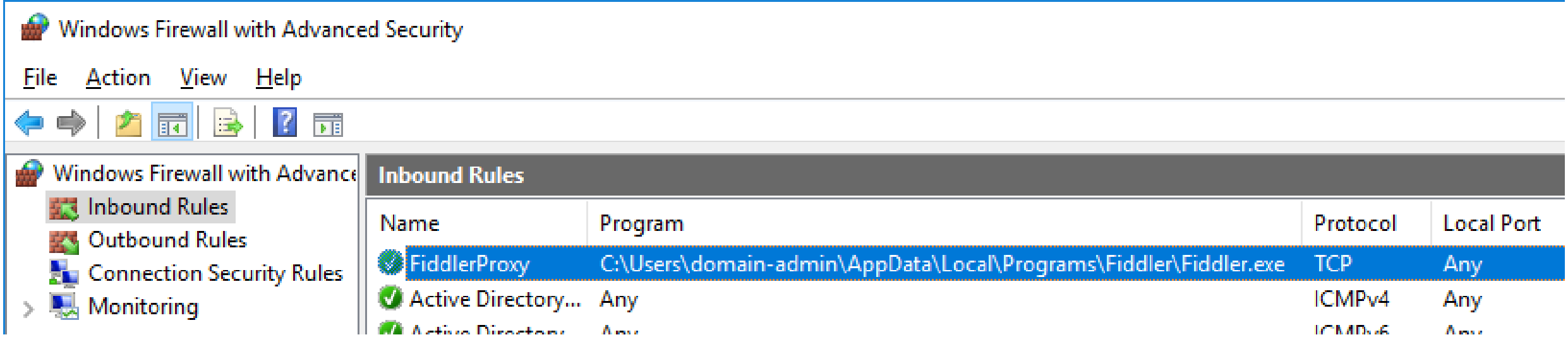
Enable remote proxy bindings



Verify remote proxy bindings

- must be 0.0.0.0:8888





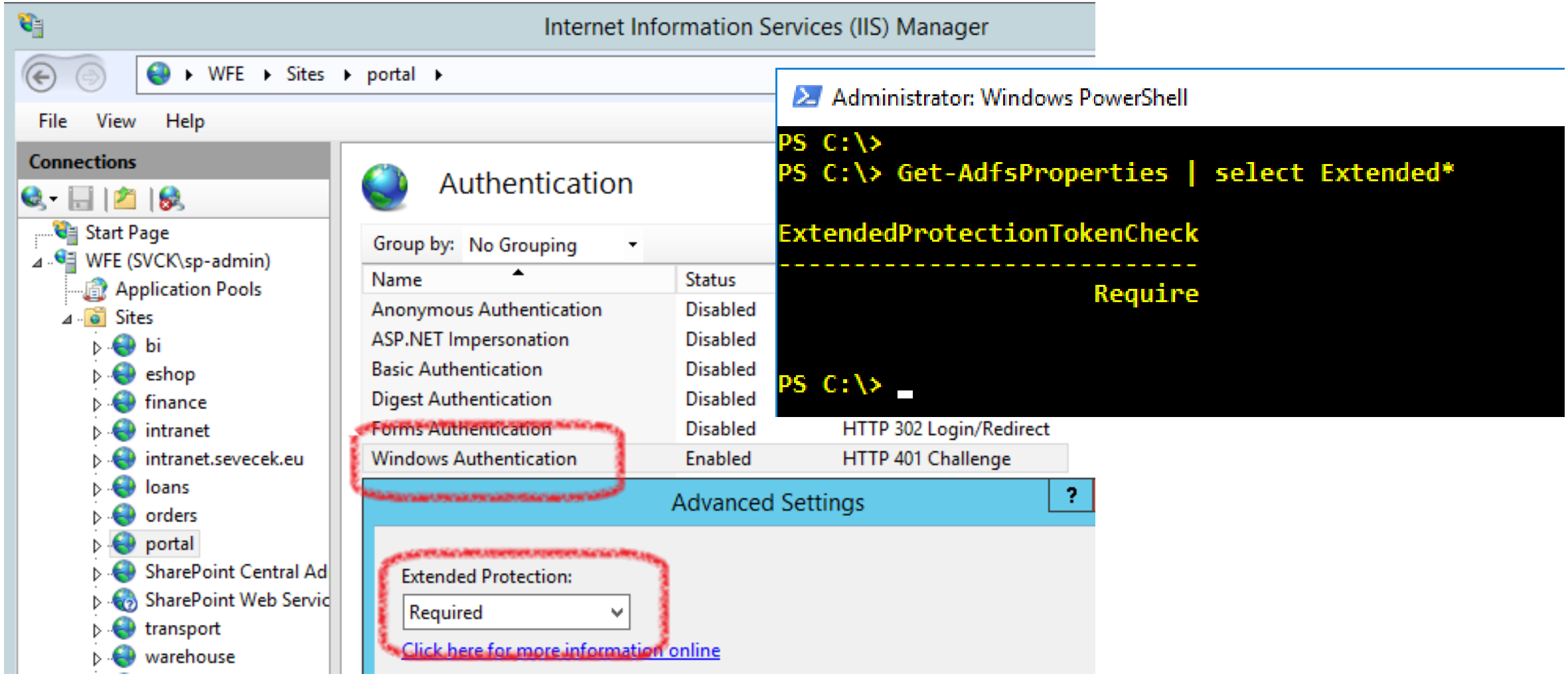
Proxy servers for more accounts and services

```
$fdl = Read-Item 'Fiddler machine name'

Set-ItemProperty 'Microsoft.PowerShell.Core\Registry::HKEY_USERS\S-1-5-
18\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"

Set-ItemProperty ' Microsoft.PowerShell.Core\Registry:: HKEY_USERS\S-1-5-
19\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"

Set-ItemProperty ' Microsoft.PowerShell.Core\Registry:: HKEY_USERS\S-1-5-
20\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"

Set-ItemProperty ' Microsoft.PowerShell.Core\Registry::
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer
"$($fdl):8888"

netsh winhttp set proxy "$($fdl):8888"
```

Testing non-browser clients

```
(New-Object Net.WebClient).DownloadString("https://www.google.com")

# Note: more examples at
# https://www.sevecek.com/Lists/Posts/Post.aspx?ID=289
```

Extended Protection for Authentication



Extended Protection on RD Gateway

- HKLM\System\CurrentControlSet\Control\LSA
  - SuppressExtendedProtection = DWORD = 3 (1 -bxor 2)

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\TerminalServerGateway\Config\Core
  - EnforceChannelBinding = DWORD = 0

Client certificate authentication

- Export .PFX with private key
- Export .CER without private key

- Import .PFX into current user profile
- Save .CER as Documents\Fiddler2\ClientCertificate.cer

Děkuji!

Ing. Ondřej Ševeček | GOPAS a.s.
ondrej@sevecek.com | www.sevecek.com

relevantní kurzy:
GOC166 (ADFS), GOC168 (IIS), GOC169 (ISO 2700x)

Aktuální a navazující kurzy sledujte na www.gopas.cz

DÁREK PRO VÁS!

Vyplňte dotazníkové hodnocení
a získejte tričko **TechEd-DevCon 2018!**

SOUTĚŽ! SOUTĚŽ! SOUTĚŽ!

Soutěžte o titul **TechEd Best Developer**
a **TechEd Best IT PRO**!